

**Course Presentation** 

# **CCNP**

(Cisco Certified Network Professional)

Certification Mapped Course
Route, Switch and Troubleshoot

**Course Presentation** 



## © 2015 Zoom Technologies India Pvt. Ltd.

All rights reserved. No part of this book or related material may be reproduced in any form or by any means without prior permission from Zoom Technologies India Pvt. Ltd. All precautions have been take to make this book and related material error-free. However, Zoom Technologies India Pvt. Ltd. is not liable for any errors or omissions. The contents of this book are subject to change without notice.

DISCLAIMER: CISCO, CCNA, CATALYST are registered trademarks of Cisco Inc.



# **Cisco Certification tracks**



CCIE

**CCNP** 

**CCNA** 

**CCENT** 

#### **CCNP Routing and Switching Version 2**

validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks





## **CCNP Module**



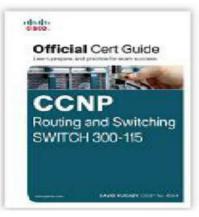
- ROUTE (300-101)
  - Implementing Cisco IP Routing
- SWITCH (300-115)
- TSHOOT (300-135)
- المحددة المحد co IP Netv

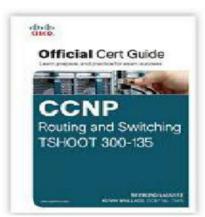


#### **Reference Books**













#### **CCNP Certification exam**



Pre-requistes:

(valid cisco CCNA Routing and Switching Certification)

Exam Details:

Register :Pearson VUE :120 minutes **Duration** 

: 45-65 questions (R&S) **Number of question** 

ologies :15-25 Question (t-shoot)

: English **Available Languages** 

: Multiple choice, Testlet, Drag and Drop, Type of Question

Simulated Lab ,Simlets

**Passing Score** : 790/1000



#### **IP Addressing**



- Zoom Technologies Two Versions of Addressing Scheme
  - IP version 4 32 bit addressing
  - IP version 6 128 bit addressing





## IPv4



• Total IPv4 Addressing Scheme is divided LAN and WAN – Unicast into 5 Classes

• CLASS A

**CLASS B** 

• CLASS C

Multicasting CLASS D

**Research and Development** • CLASS E



## IPv4



Class	Range	Octet Format	Subnet Mask	Cisco / Notation
Class A	0.0.0.0 to 127.255.255.255	N.H.H.H	255.0.0.0	/8
Class B	128.0.0.0 to 191.255.255.255	N.N.H.H	255.255.0.0	/16
Class C	192.0.0.0 to 223.255.255.255	N.N.N.H	255.255.255.0	/24
Class D	224.0.0.0 to 239.255.255.255	N/A	N/A	N/A
Class E	240.0.0.0 to 255.255.255	N/A	N/A	N/A





## What is a Router?



- A Router is a internetworking Device.
- It routes the packet from one logical network to another logical network
- It has two main functions.
  - Determination of best path towards destination.
  - Switching packet from inbound interface to outbound interface.





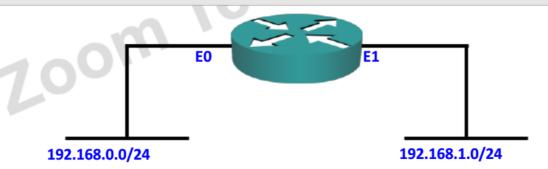
## **Routing**



- Forwarding the packet from one network to other network.
- Routing is enabled by default

To enable or disable IP Routing

Router(config)# [no] ip routing







## **Types of Routing**



- Static Routing
- Dynamic Routing





## **Static Routing**



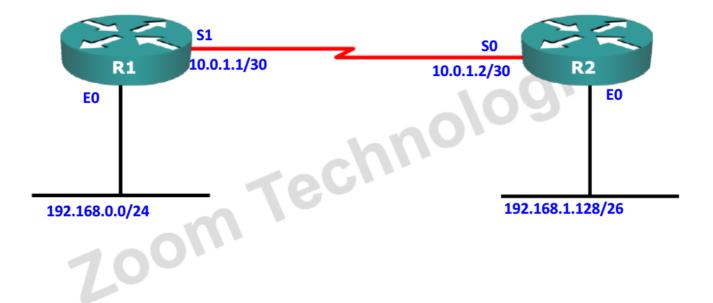
- · Manually configured by Administrator
- Administrative distance is 1
- Destination network should be known
- ace dies Routing based on next hop IP address or exit interface
- · Secure and fast





# **Static Routing Configuration**







#### **Static Default Route**

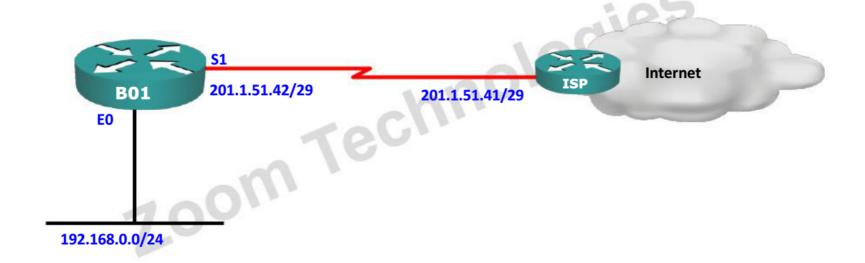


- Static default route will be used for unknown destinations
- It may be used for accessing the Internet.
- It can be also used on a Stub router.
- It is least preferred route in the routing table.
- The router uses this route only when it cannot find a more suitable match in the routing table.



# Default route configuration.

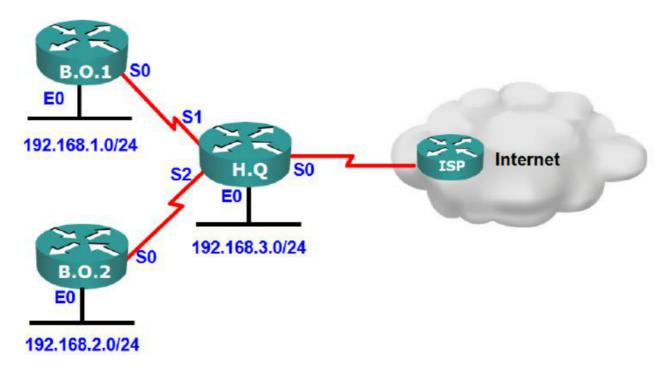






# **Static and Default routing Example**

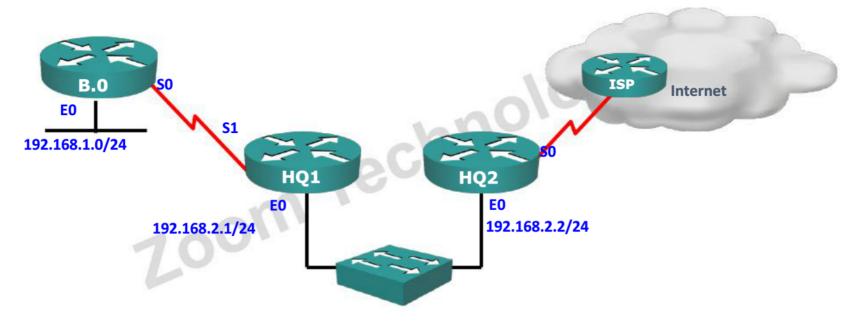






# Static and Default Route configuration







## **Floating Static Route**



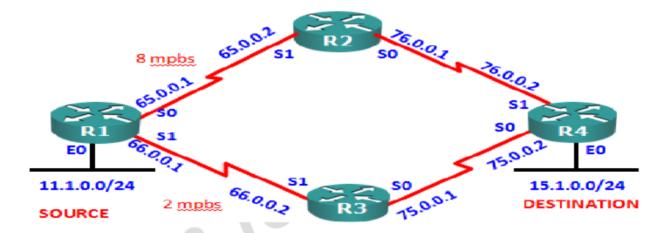
- Floating static routes are static routes that are used to provide a backup path to a primary static route, in the event of a link failure.
- The floating static route is only used when the primary route is not available.
- To accomplish this, the floating static route is configured with a higher administrative distance than the primary static route.





## **Floating Static Route**





**Floating Static Route Configuration** 

R1(config)# ip route 15.1.0.0 255.255.255.0 65.0.0.2

R1(config)#ip route 15.1.0.0 255.255.255.0 66.0.0.2 7



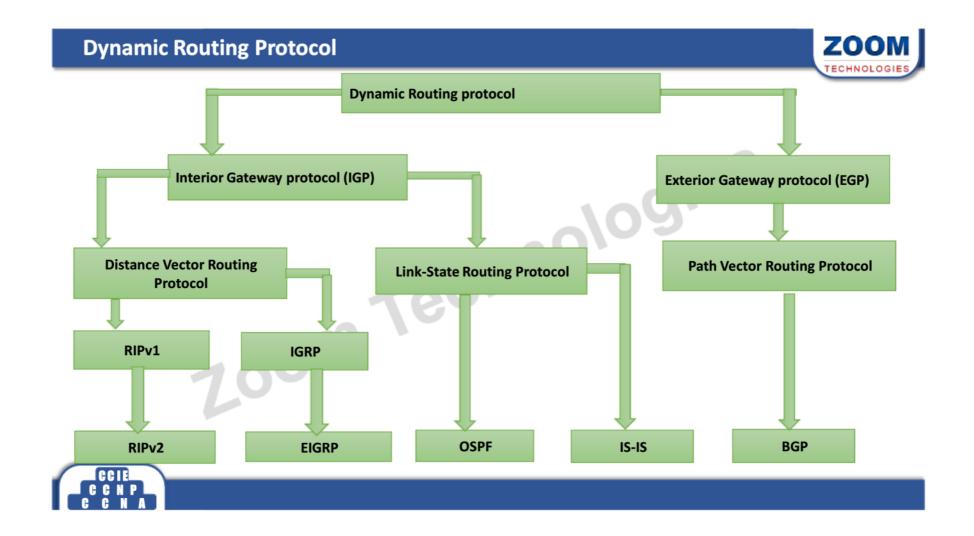
## **Dynamic Routing Protocol**



- Dynamic routing protocols, exchange routing information with the neighbors and build the routing table automatically
- Administrator need to advertise only the directly connected networks
- Any changes in the network topology are automatically updated







## **Types of Dynamic Routing Protocols**



- Distance Vector Routing Protocol (RIP,IGRP)
- Link State Routing Protocol (OSPF,IS-IS)
- Zoom Technologies Advanced Distance Vector Routing Protocol (EIGRP)
- Path Vector Protocol (BGP)





#### **Summarization**



- Combining the contiguous address into one and advertising to neighbor Router
  - Advantages
  - Minimizing the routing table entries
  - uth les Less use of resources like memory, processor, bandwidth
  - Less number of updates
- There are two type of Summarization
  - Auto summary
  - Manual summary



## **Auto Summary**



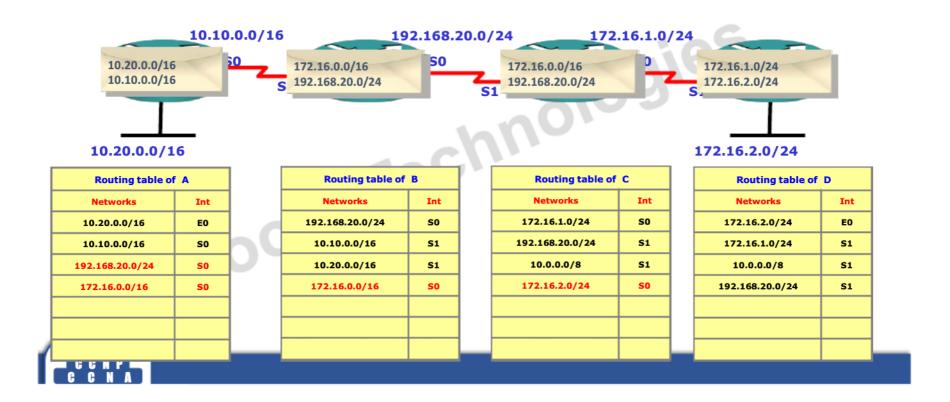
- · Subnet at major network boundary will be summarized into class full updates
- A Class full routing protocol does auto summary by default and it cannot be turned off
- Routing protocols like RIPv2, EIGRP, BGPv4 support auto summary
- . support a Link state routing protocol i.e. OSPF and ISIS do not support auto summary





## **Auto Summary**





## **Manual summary**

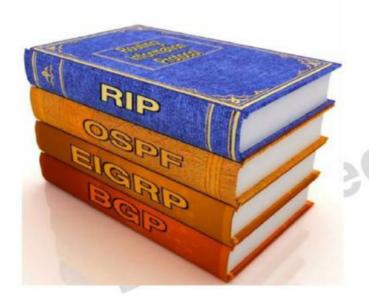


- Administrator manually configures Summarization
- Zoom Technologies Summary address contains networks in 2n subnets (FLSM)
- · It is supported by all classless routing protocols



# **Routing Protocol Selection**













#### **EIGRP Features**



- Open Standard
- Advanced distance-vector routing protocol
- Diffusing update algorithm (DUAL)
- Administrative distance is 90-internal, 170-external
- Classless
- logies Support FLSM, VLSM, CIDR, Auto and Manual summary
- Metric = composite metric (32 bits)
  - Bandwidth, load, delay, reliability
- Updates are sent as multicast(224.0.0.10) or unicast



#### **EIGRP Features**



- Incremental / triggered update
- Very fast convergence
- Max hops = 255 (default is 100 hops)
- Load balancing on 4 equal cost paths (Default)
- rechnologie<sup>5</sup> Max 16 paths (equal or unequal cost paths)
- It supports multiple routed protocols
  - (IP, IPX, Apple Talk)
- EIGRP uses protocol no 88 room



## **Key Technologies of EIGRP**



- Neighbor discovery

- Protocol Dependent Modules (PDM)

7.00m T



#### **EIGRP Tables**



- Neighbor table List of directly connected routers running EIGRP in same autonomous system
- Topology Table aghbors...ation List of all routes learned from its directly connected neighbors outing table
- Routing table List of best paths towards each destination





# **Components of EIGRP**



- Link Local Distance -- Distance from Router to Neighbor Router
- Advertised Distance Distance from Neighbor Router to Destination
- Feasible Distance -- Link Local Distance + Advertised Distance
- Successor -- Best Path to reach destination
- Feasible Successor -- Second Best Path to reach destination



# **EIGRP Tables**



	Neighbo	or Table of Rou	ter A	
Neighbor Interface				
В	B S0			
С	:		S1	
	Topolog	y Table of Rou	ter A	
Network	NH	AD	FD	
	В	1000	2000	s
10.0.0.0/8	С	1500	2500	
	Routin	g Table of Rout	ter A	
Network		Next Hop		FD
10.0.0.0/8 B		2	000	





#### **EIGRP** metric calculation



dies

- EIGRP Metric
- = [K1 \* BW + ((K2 \* BW) / (256 load)) + K3 \* delay]



· Formula with default K values

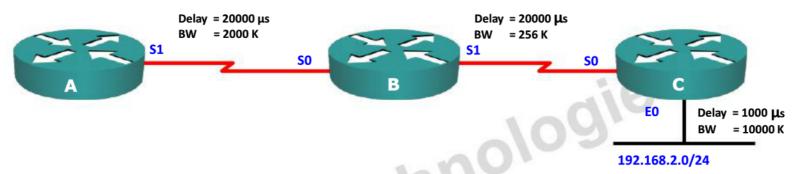
$$(K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0)$$

- EIGRP Metric
- BW = (107/lowest Bandwidth in kbps)\*256
- Delay = (sum of total delay/10)\*256



## **EIGRP Metrics Calculation Example**





- Delay is the sum of all the delays of the links along the paths:
  - Delay = [delay in tens of microseconds]  $\times$  256
- Bandwidth is the lowest bandwidth of the links along the paths:

Bandwidth =  $[10,000,000 / (bandwidth in kbps)] \times 256$ 

A → 192.168.2.0

Least bandwidth 256 kbps

Total delay 41,000

Composite Metric =  $[[10000000/256] \times 256] + [[41000/10] \times 256]$ 

= 10000000 + 1049600 = 11049600

C C N P

#### **EIGRP Packets**



#### **Hello Functions**

- Neighbor Discovery
- Neighbor Formation
- Keep Alive

#### **Update**

· To exchange routing information with neighbor

#### Query

 Query message is generated when successor is down & Feasible Successor not available

ologies

#### Reply

Reply Message is sent in response to query message

#### **ACK**

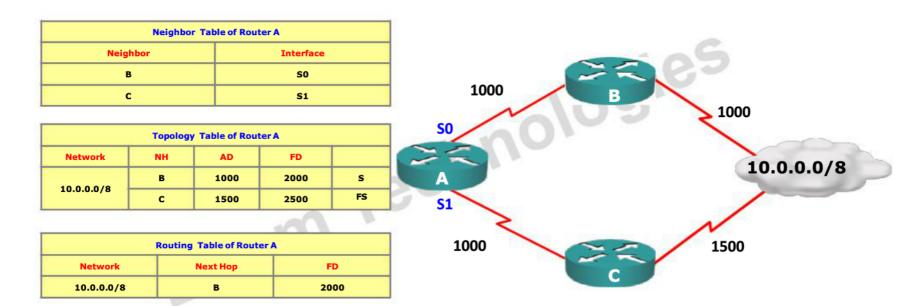
For every Update, Query and Reply router will generate ACK message



## **Initial Route Discovery** ZOOM TECHNOLOGIES Hello Neighbor Table Neighbor Table Hello (2) Update (4) 4 Topology Table Topology Table (3) (5) **Update** ACK Routing Routing Table Table

# **Diffusing Update Algorithm - DUAL**





## Feasibility Condition = Second best AD < FD of Successor



## **DUAL**



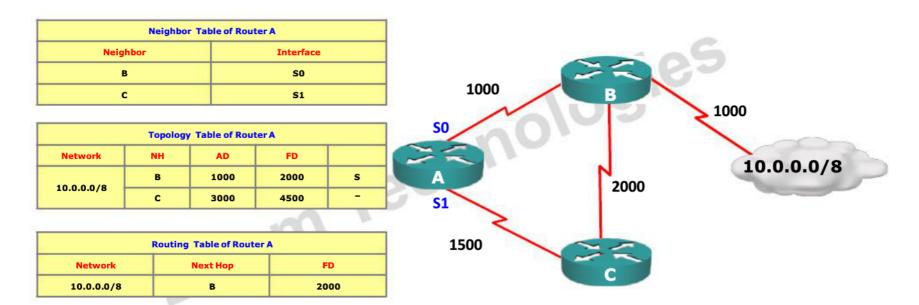
	Neighbo	r Table of Rout	ter A	
Neighbor Interface				
B 50				
с		S1	S1	
	Topolog	y Table of Rout	ter A	
Network	NH	AD	FD	
40.000/0	—в	1000	2000	s-
10.0.0.0/8	С	1500	2500	s
			-	1
	Routing	Table of Rout	er A	
Network		Next Hop	F	FD
10.0.0.0/8		С	25	500





## **DUAL**





#### Feasible Successor = Second best AD < FD of Successor



## **DUAL**



	Neighbo	r Table of Rout	ter A	
Neighbor Interface				
В	B 50			
С			S1	
	Topolog	y Table of Rout	ter A	
Network	NH	AD	FD	
	—в	1000	2000	s
10.0.0.0/8	С	3000	4500	S
			-00	1
	Routing	Table of Rout	er A	
Network		Next Hop	F	D O
10.0.0.0/8		С	45	00





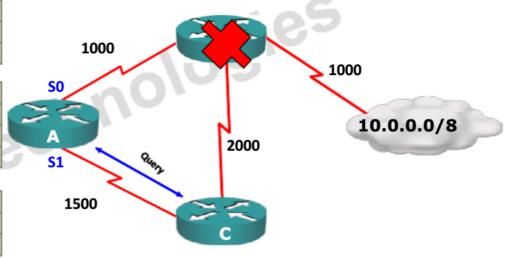
## **DUAL**



Neighbor Table of Router A			
Neighbor	Interface		
<u>B</u>	so		
С	S1		

	Topolog	y Table of Rout	er A	
Network	NH	AD	FD	
	В	1000	2000	S
10.0.0.0/8		3000	4500	

Routing Table of Router A				
Network	Next Hop	FD		
10.0.0.0/8	<u> </u>	2000		



LAUP



# **Configuring EIGRP**



To enable EIGRP as the IP routing protocol.

Router(config)# router eigrp <AS No.>

Identify attached networks participating in EIGRP.

Router(config-router)# network network-id [wildcard-mask]

Defining the interface's bandwidth for the purposes of Metric calculation Router(config-if)# bandwidth <kilobits>



## **EIGRP Queries**

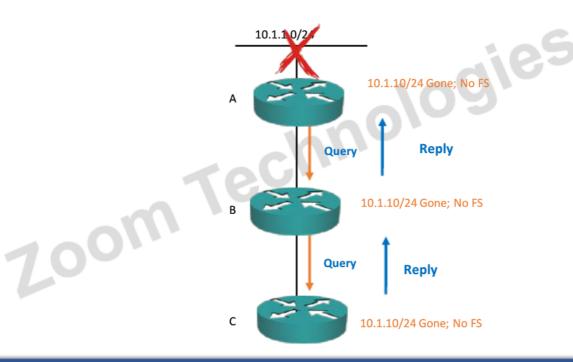


- Router loses a best path and does not have a FS (Second best path) in its topology table, it looks for an alternate path to the same destination, this is called as Active state for that route.
- If a router does not have an alternate route, it queries each of its own neighbors



# **EIGRP Queries**









## **Stuck In Active**

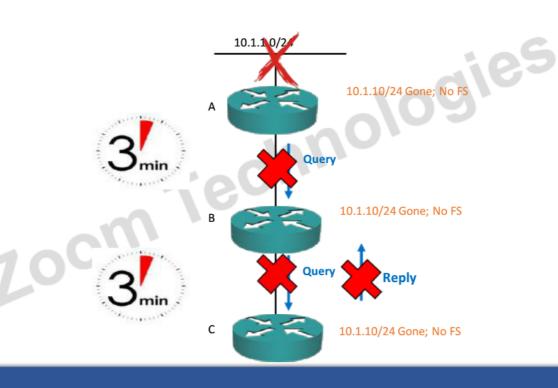


- The most common reasons for SIA routes are as follows:
  - The router is too busy to answer the query
  - · The link between the two routers is not good
  - I ne link between the two routers is not good
     A failure causes traffic on a link to flow in only one direction.



## **Stuck In Active**









## **Preventing SIA**



- Cisco IOS Software Release 12.1(5) and later, with the Active Process Enhancement feature.
- This feature enables an EIGRP router to monitor the progression of the search for a successor route and ensure that the neighbor is still reachable.



#### **EIGRP Stub**



- EIGRP stub is a special router which will not receive Query messages.
- A stub router informs its status to all other neighbors.
- EIGRP stub routing reduces CPU utilization on the router.
- EIGRP stub routing mainly implemented in hub and spoke environment.





## **Summarization**

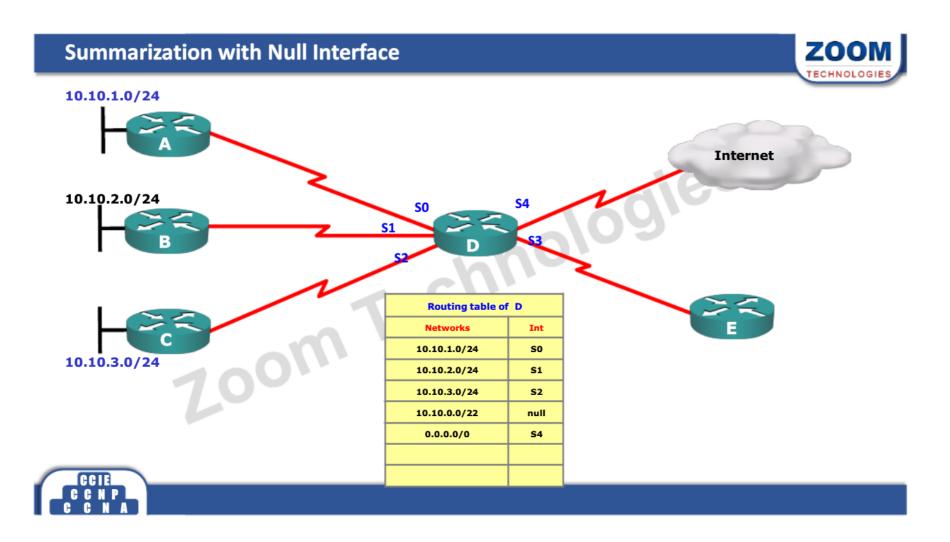


- Auto summary
  - EIGRP does auto summary at major logical network boundary
- Manual summary
  - EIGRP supports manual summary on a per interface basis
- Summary will be continued till the last specific route goes down
- · Summary metric will be the best metric from specific route

700m

· Router of the summary route will create a summary route pointing to null interface





## **Configuring EIGRP Route Summarization**



Turns off automatic summarization for the EIGRP process

Router(config-router)# no auto-summary

room

Creates a summary address that this interface will generate.

Router(config-if)# ip summary-address eigrp <as-number> <address> <subnet mask>



## **EIGRP Load Balancing**



- Routes with lowest equal metric are installed in the routing table (equal-cost load balancing)
- There can be up to sixteen entries in the routing table for the same destination:
  - The number of entries is configurable
  - · The default is four
- Variance is configured for unequal cost load balancing
  - Variance is the multiplier to FD of successor
  - Default is 1(equal cost load balancing)

700m





# **EIGRP Unequal-Cost Load Balancing**



Allows the router to include routes with a metric smaller than the multiplier value times the metric of successor

Router(config-router)# variance <multiplier>



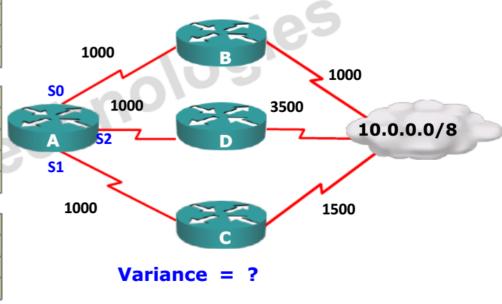
## **Variance Example**



Neighbor Table of Router A		
Neighbor	Interface	
В	S0	
с	S1	
D	S2	

		Topology	Table of Rou	ter A	
I	Network	NH	AD	FD	
		В	1000	2000	s
	10.0.0.0/8	С	1500	2500	FS
		D	3500	4500	-

		Routing Table of Router	A	
	Network	Next Hop	FD	
	10.0.0.0/8	В	2000	
		С	2500	



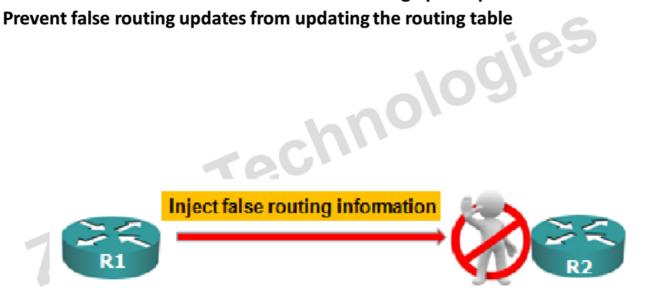




#### **Router Authentication**



- Gives greater security to the routing protocol by supporting authentication
- A router authenticates the source of each routing update packet that it receives.
- Prevent false routing updates from updating the routing table

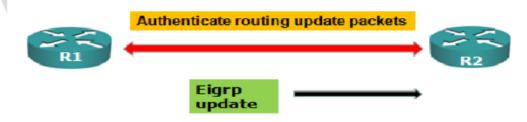




#### **Router Authentication**



- Many routing protocols support authentication
- Router authenticates the source of each routing update
- ;hnologies · Simple password authentication is supported by:
  - IS-IS
  - OSPF
  - RIPv2
- MD5 authentication is supported by:
  - OSPF
  - BGP
  - EIGRP







#### **MD-5 Authentication**



- MD-5 authentication uses key-chains to perform routing protocol authentication.
- Each and every Key Chain contains 1 or more keys.
- Each and Every key identified using Key number and key-string.
- Key number and key-string need to match on both the routers.





## **MD-5 Authentication Configuration**



- Step1: Create key Chain on the router
- Router(config)# key chain zoom
- Router(config-keychain)#key 1
- Router(config-keychain-key)#key-string ccnp
- Router(config-keychain-key)#exit
- ologies Step 2: Apply Key Chain on the Interface that is connected to neighbor
- R1(config)# key chain zoom
- R1(config-keychain)#key 1
- R1(config-keychain-key)#key-string ccnp
- R1(config-keychain-key)#exit







#### **OSPF Features**



- Open standard (IETF)
- SPF or Dijkstra algorithm
- Link-state routing protocol
- Classless
  - Supports FLSM, VLSM, CIDR and Manual summary
- Incremental / triggered updates
- Updates are sent as multicast (224.0.0.5 and 224.0.0.6)
- Metric = Cost (cost = 108/bandwidth in bps)
- Administrative distance = 110
- Load balancing via 4 equal cost paths by default (unequal cost load balancing not supported)





## **Link-state Routing Protocol**



- Auto Neighbor discovery
- Hierarchical network design
- Sends periodic updates, known as link-state refresh, every 30 minutes
- area Maintains similar database on all the routers within an area
- · Router ID is used to identify each router



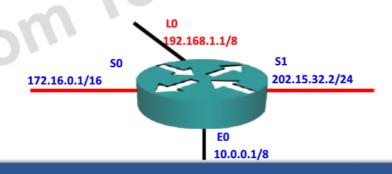
#### **Router ID**



- Highest IP address on Active Physical Interface
- Highest IP address on Logical Interface (if configured)
- · Highest preference is for Router ID command

# 10gies **Configuring Router ID**

Router(config-router)# router-id <ip address>





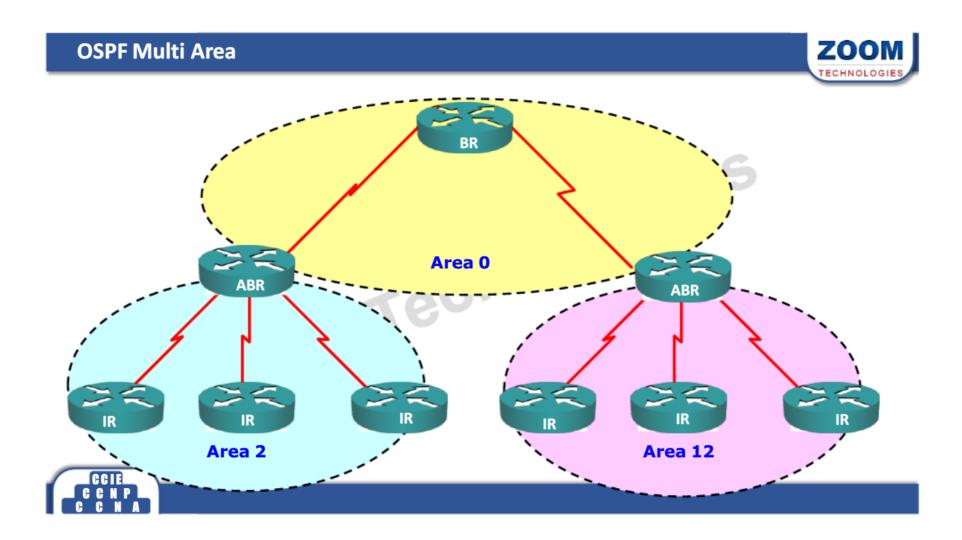


### **Link-State Data Structure : Network Hierarchy**



- Link-state routing has a hierachical network
- Zoom Technologies • This two-level hierarchy consists of the following:
  - Transit area (backbone or area 0)
  - Regular areas (nonbackbone areas)





### **Types of Routers in ospf**



- Backbone router- The router which belongs to backbone area is called as Backbone router
- Internal Router- The router which belongs to regular area is called Internal Router
- ABR-The router which shares two different areas is called Area Border Router
- ASBR- The router which is connected to different protocol is called Autonomous system boundary router.



### **Link-State Data Structures**



- Neighbor Table
  - Also known as the adjacency database
  - Contains list of recognized neighbors
- Database Table
  - Typically referred to as LSDB
  - Contains information about all routers and their attached links in the area or networks
- Routing Table
  - Commonly named as forwarding database
  - Contains list of best paths to each destination





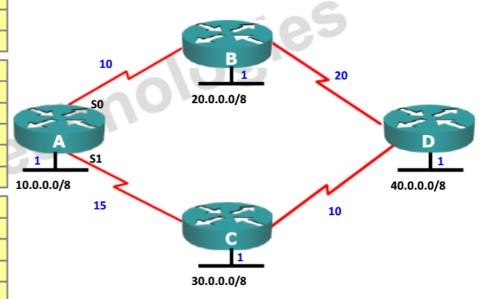
### **OSPF Database**



Neighbor Table of Router A			
	Neighbor	Interface	
В		S0	
	С	S1	

Link State Data base of Router A				
Router	Links			
A	5			
В	5			
С	5			
D	5			

	Routing Table of Router A			
Network	Next Hop	Cost		
20.0.0/8	В	11		
30.0.0/8	С	16		
40.0.0.0/8	С	26		





### **OSPF Metric calculation**



- OSPF metric is not defined in standards
- Every vendor uses a different formula to calculate metric
- OSPF Metric in Cisco = Cost = 108 / Bandwidth in bps
- Ex:

•	Serial link	64 Kbps	cost =1562
•		1544 Kbps	cost = 64
•		2000 Kbps	cost = 48
•	Ethernet	10 Mbps	cost = <b>10</b>
•	FastEthernet	100 Mbps	cost = 1
•	<b>Gigabit Ethernet</b>	1000 Mbps	cost = 1

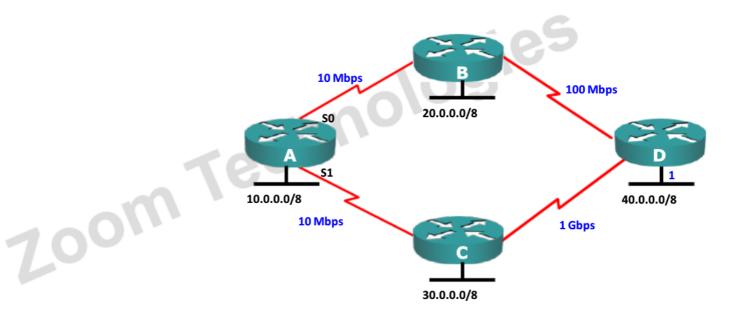




### **OSPF Cost calculation**



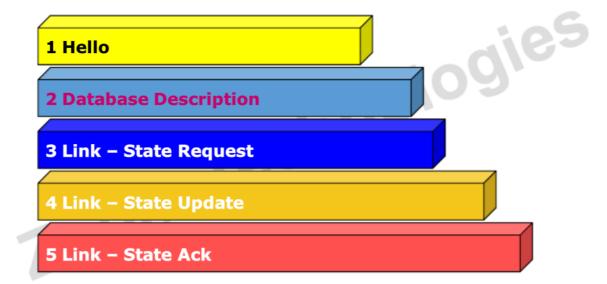
How much does it cost to reach 40.0.0.0/8 from Router A





### **OSPF Packet Types**



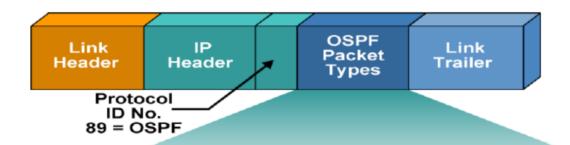






### **OSPF Packet Header Format**



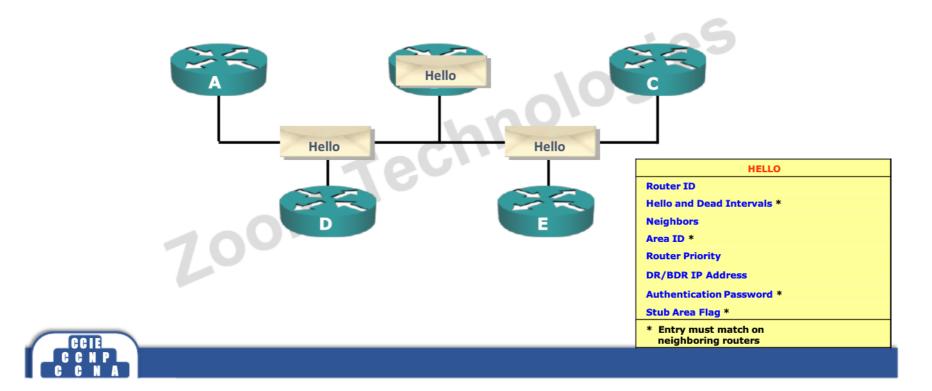


									/
OSPF Packet									
Version Number	Туре	Packet Length	Router ID	Area ID	Check- Sum	Authen- tication Type	Authen- tication	Data	



### **OSPF Neighbor relationship**





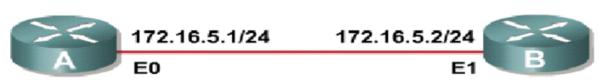






### **Establishing bidirectional Communication**

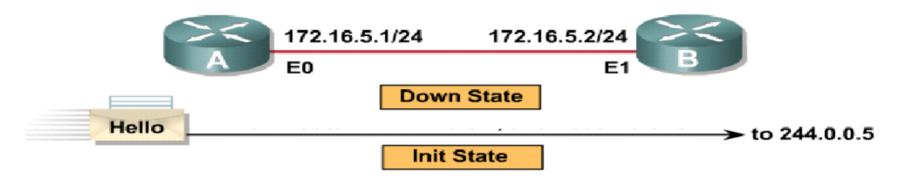




Down State



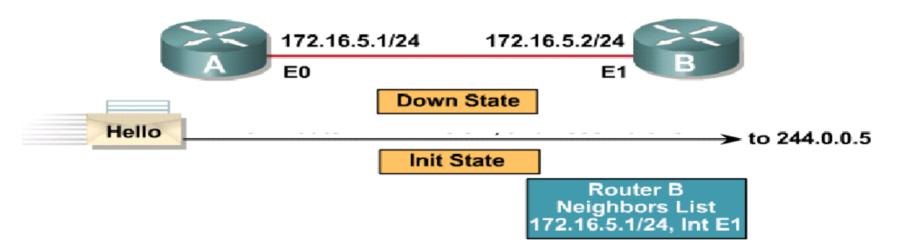




### C C N A

### **Establishing bidirectional Communication**

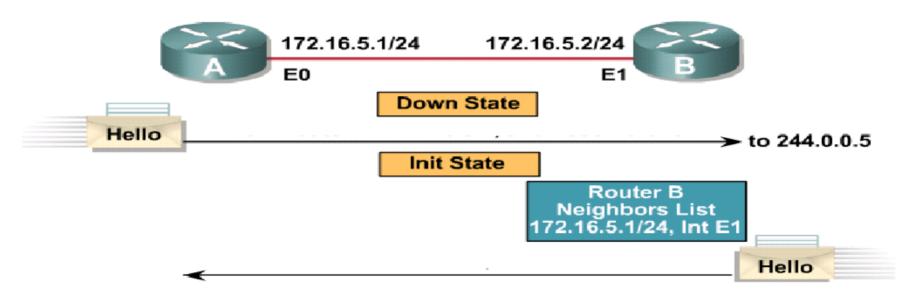








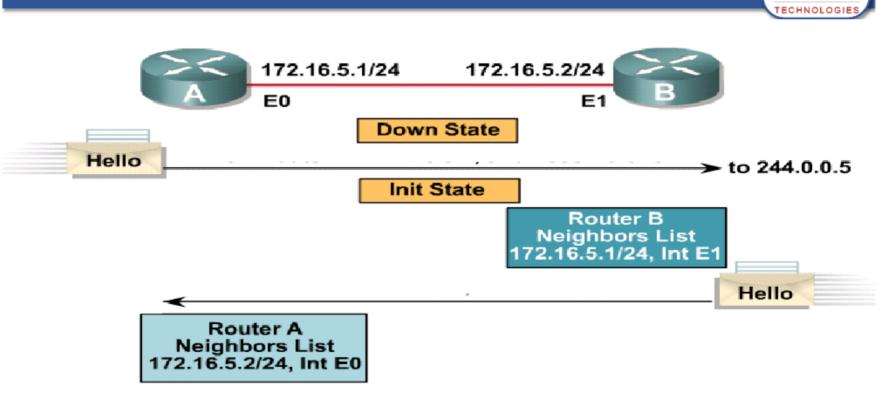




### C C N A

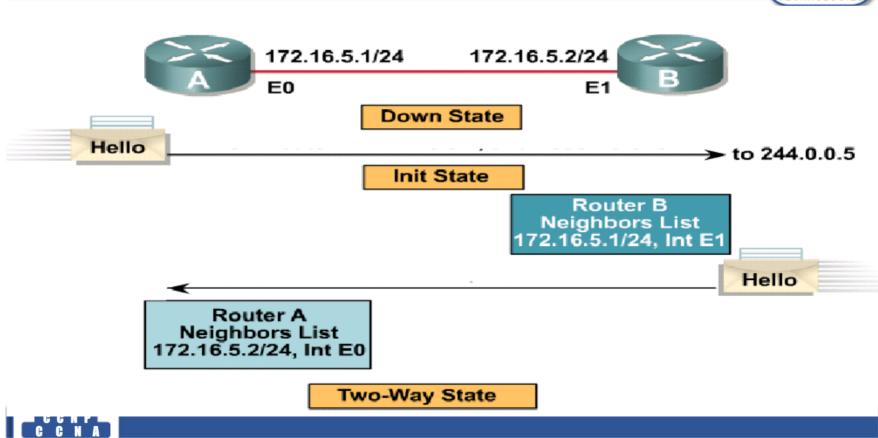
### **Establishing bidirectional Communication**











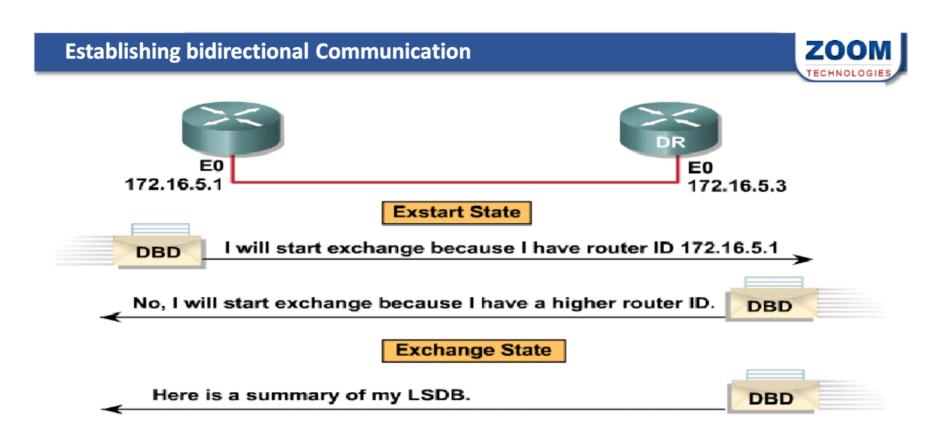
### Establishing bidirectional Communication Technologies 172.16.5.1 Exstart State Hello I will start exchange because I have router ID 172.16.5.1







### CCNP





## Establishing bidirectional Communication DR ED 172.16.5.1 Exstart State Hello I will start exchange because I have router ID 172.16.5.1 No, I will start exchange because I have a higher router ID. Exchange State Here is a summary of my LSDB. DBD Here is a summary of my LSDB.





### Establishing bidirectional Communication ZOOM TECHNOLOGIES 172.16.5.1

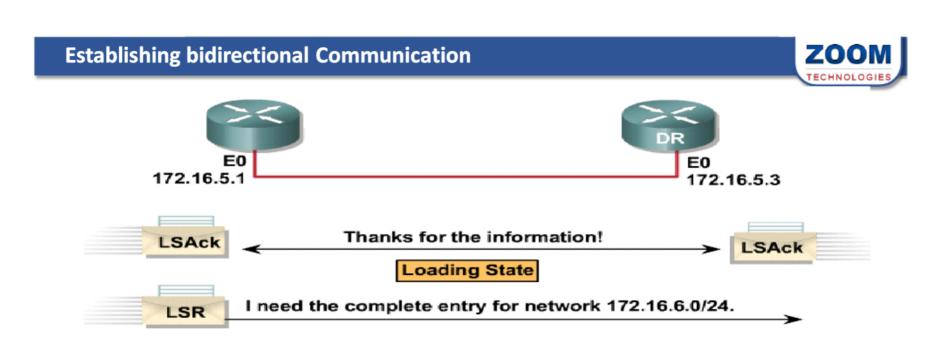
Thanks for the information!

**Loading State** 

LSAck

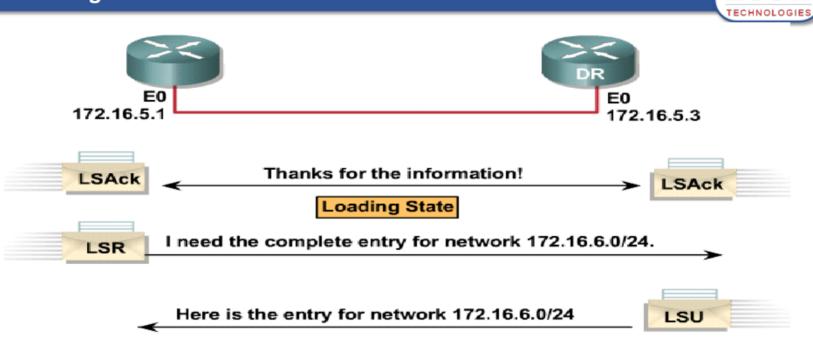
### LUUNPL

LSAck

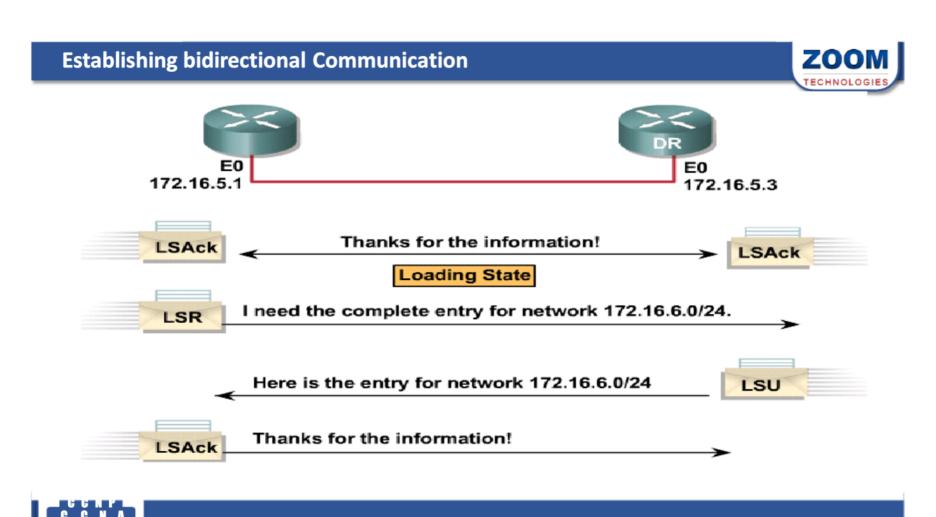


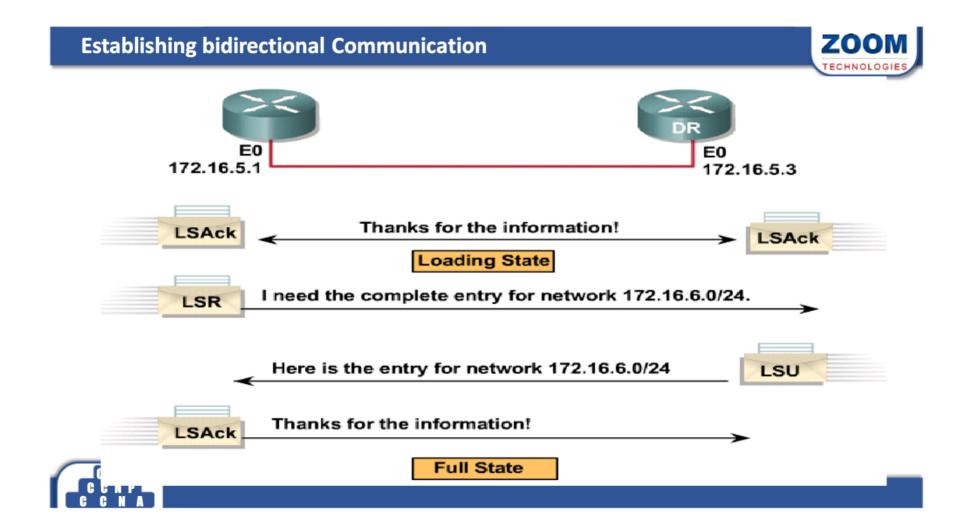


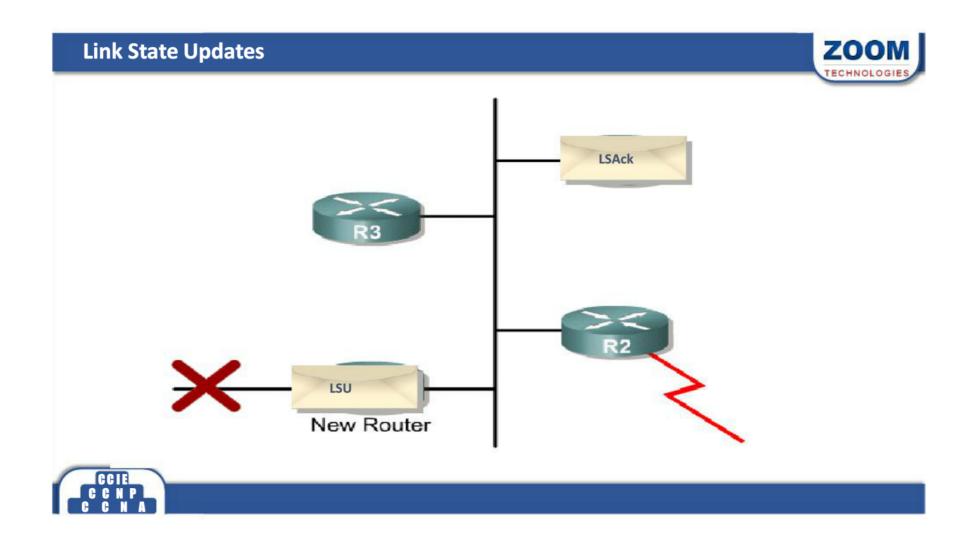




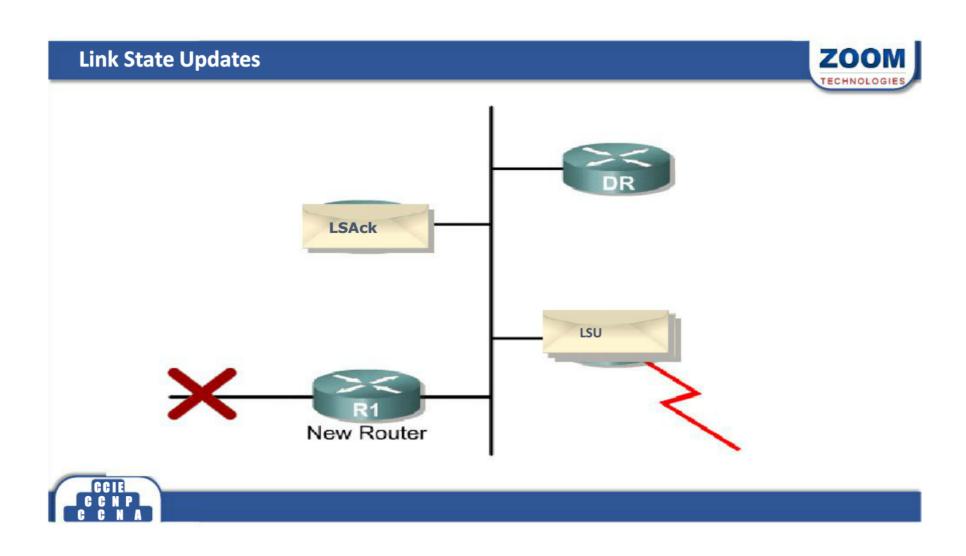
### C C N A







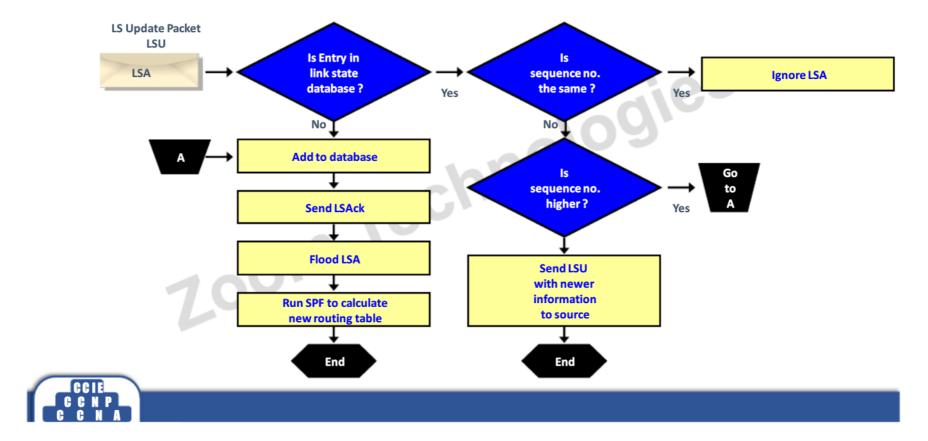
### Link State Updates R3 R2 R2 New Router



CCIE CCNP CCNA

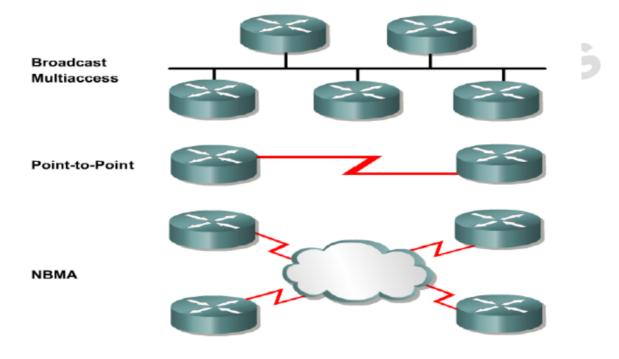
### **LS Data Structures: LSA Operation**





### **OSPF Network Types**





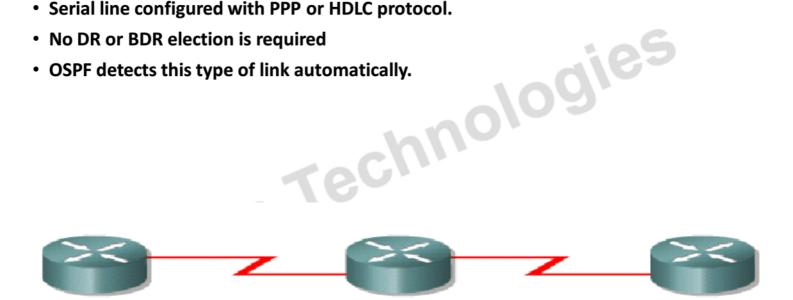




### **Adjacency Behavior for a Point-to-Point Link**



- A point-to-point link is a single pair of routers.
- Serial line configured with PPP or HDLC protocol.
- No DR or BDR election is required
- OSPF detects this type of link automatically.





### **Broadcast Multi Access**



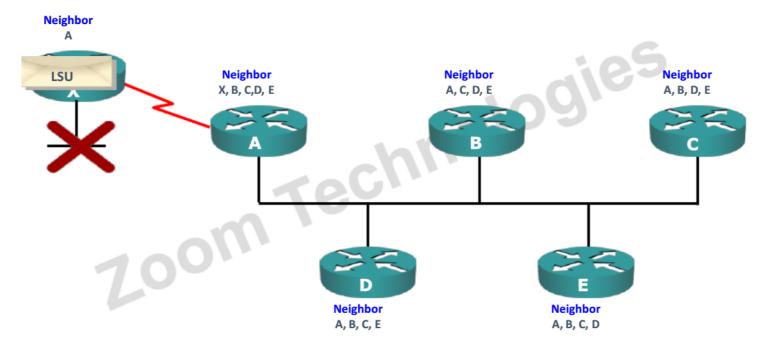
- Topology like Ethernet and Token Ring is BMA.
- DR and BDR Election is required.
- Zoom Technologies OSPF detects this type of link automatically



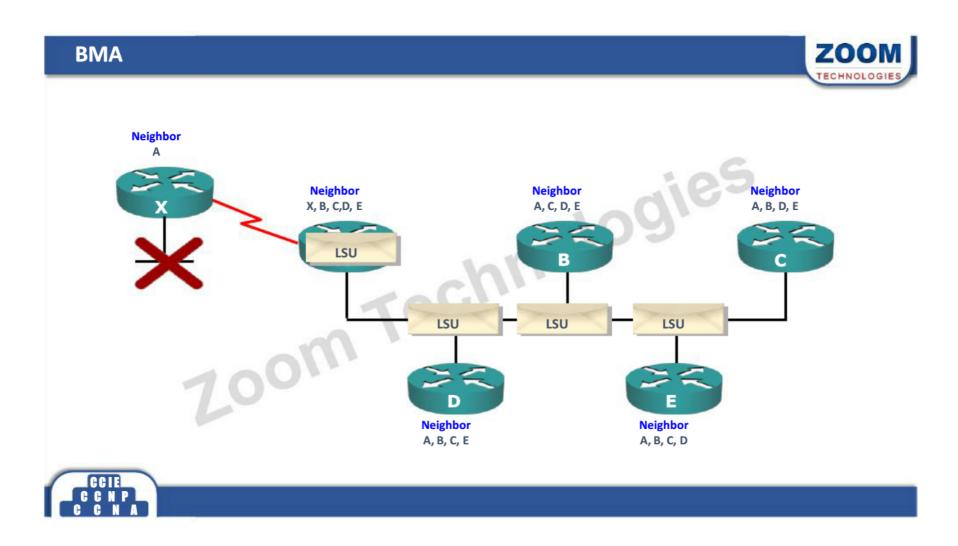


### **BMA**





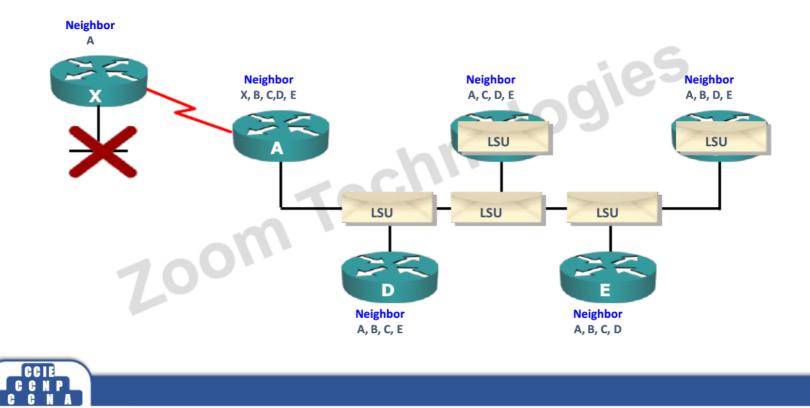


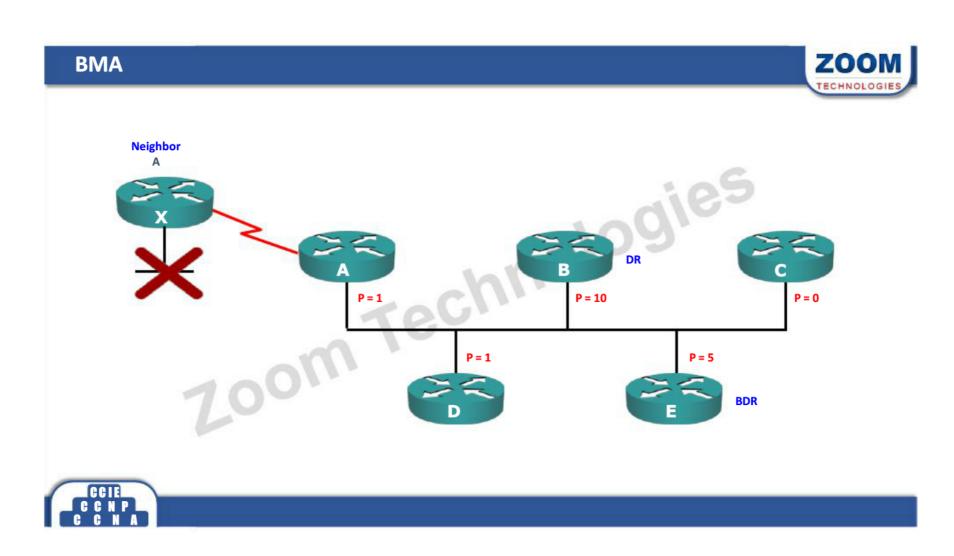




### **BMA**







### **Designated Router and Backup Designated Router**



- The router with the highest priority is DR
- The router with second-highest priority is BDR
- The default priority value is 1
- In the case of a tie, the router with highest router ID becomes DR, the second highest router ID becomes the BDR
- If router priority is 0 it cannot become the DR or BDR
- Router which is not a DR or BDR is called as DROTHER
- DR and BDR election is not preemptive
- We can manually set the priority to force a router to become the DR.



### **DR/BDR Elections**



,10gies

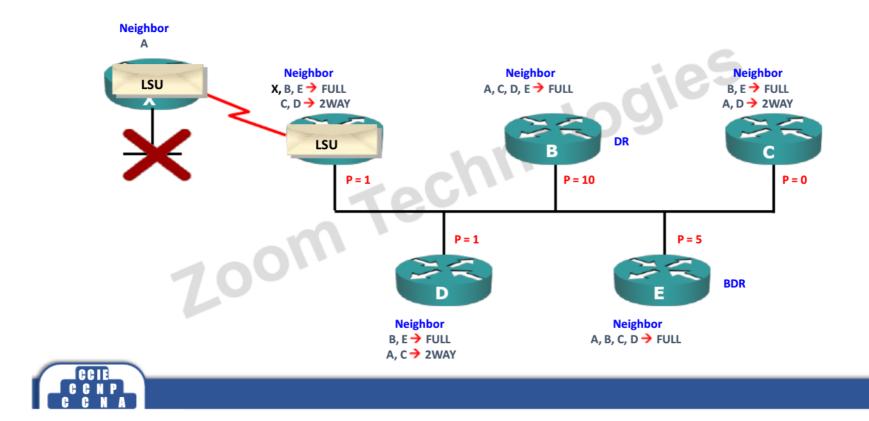
- Neighbors
- DR/BDR → DROTHER → Full
- DROTHER → DR/BDR → Full
- DROTHER → DROTHER → 2 Way
- Updates
- DROTHER → DR/BDR → 224.0.0.6
- DR → DROTHER → 224.0.0.5

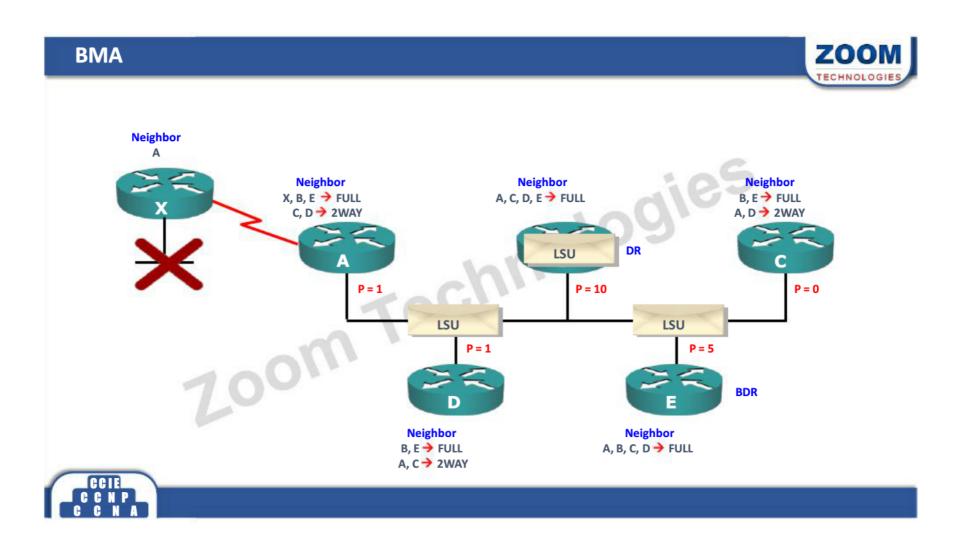
7.00m







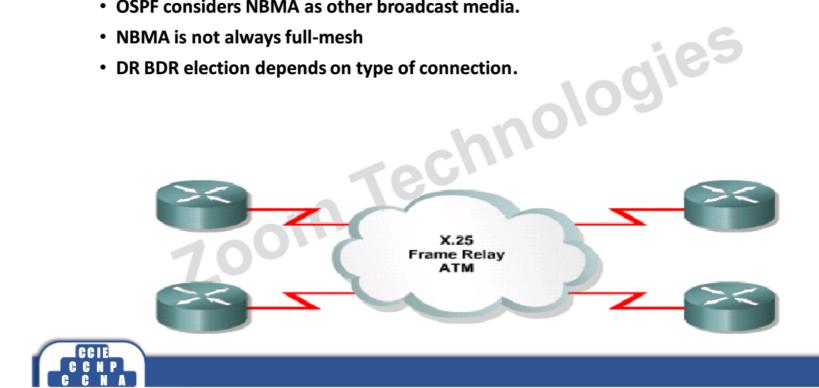




### **NBMA**



- Links like Frame relay, ATM and X.25.
- · OSPF considers NBMA as other broadcast media.
- NBMA is not always full-mesh
- DR BDR election depends on type of connection.



### **NBMA Types**



OSPF Mode	Adjacency	Configured	Hello Timer	RFC or Cisco
Broadcast	DR/BDR	Automatic	10 sec	Cisco
Nonbroadcast (NBMA)	DR/BDR	Manual	30 sec	RFC
Point-to-Multipoint	No DR/BDR	Automatic	30 sec	RFC
Point-to-Multipoint Nonbroadcast	No DR/BDR	Manual	30 sec	Cisco
Point-to-Point	No DR/BDR	Automatic	10 sec	Cisco







### Why Multiarea OSPF?



- · Single-area OSPF is useful in smaller networks. If an area becomes too big, the ations and the second s following issues must be addressed:
- Large routing table
- Large link-state database (LSDB)
- Frequent SPF algorithm calculations

7.00m

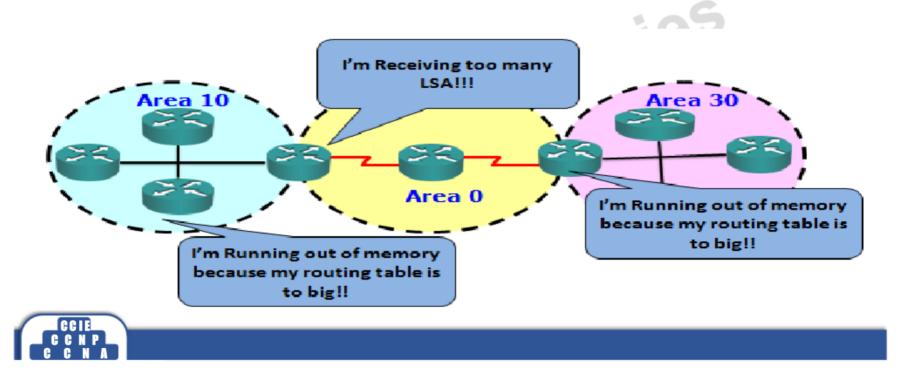




### **Multi Area OSPF**

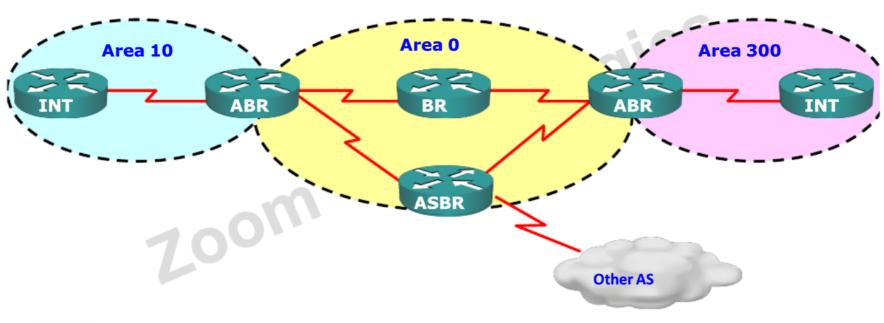


Multiarea OSPF requires a hierarchical network design and the main area is called the backbone area, or area 0, and all other areas must connect to the backbone area.



### **Type of OSPF Routers**











### **Benefits Of Route Summarization**

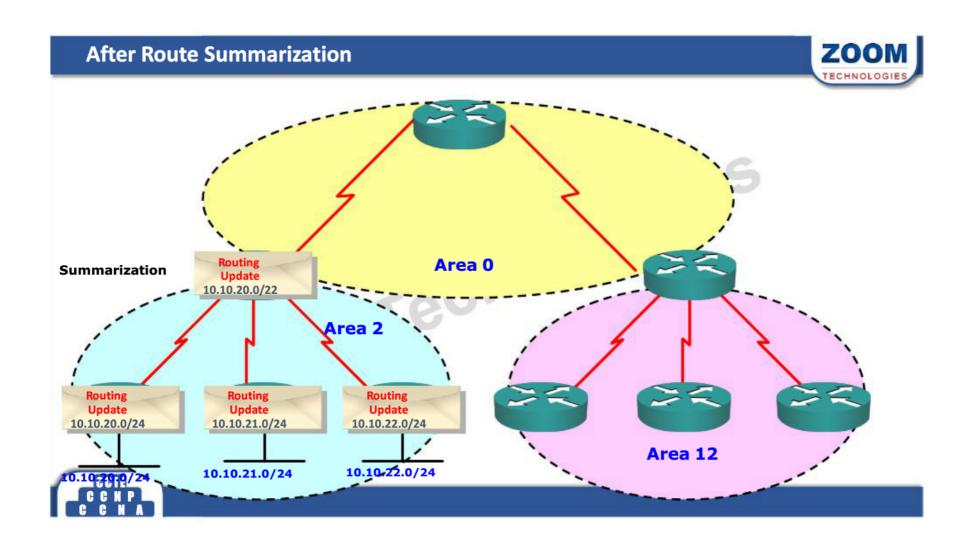


- · Minimizes number of routing table entries
- Localizes the impact of a topology change
- Zoom Technologies Reduces LSA 3 and 5 flooding and saves CPU resources





# Routing Update 10.10.22.0/24 Routing Update 10.10.22.0/24 Area 2 Routing Update 10.10.22.0/24 O.10743177/29 O.1074317/29 O.1074317/29



### **Types Of LSA**



LS Types	Name
1	Router LSAs
2	Network LSAs
3	Summary LSAs
4	ASBR Summary
5	Autonomous System External LSAs
6	Multicast OSPF LSA
7	Defined for not-so-stubby areas



### LSA Type 1: Router LSA



ologies

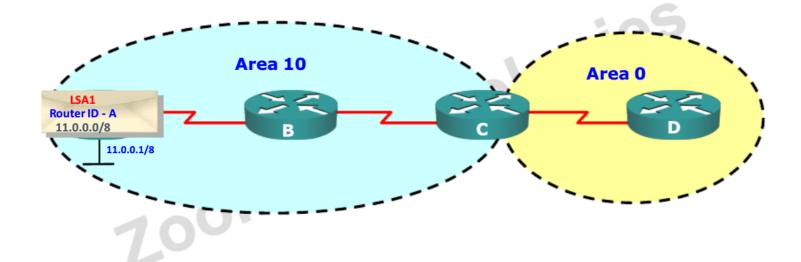
- One Router LSA (type 1) for every router in an area
  - · Includes list of directly attached links
  - Each link identified by IP prefix and link type
- Identified by the router ID of the originating router
- ute.
  ..uss the ABR • Floods within its area only; does not cross the ABR





### **LSA Type 1: Router LSA**







### **LSA Type 2: Network LSA**



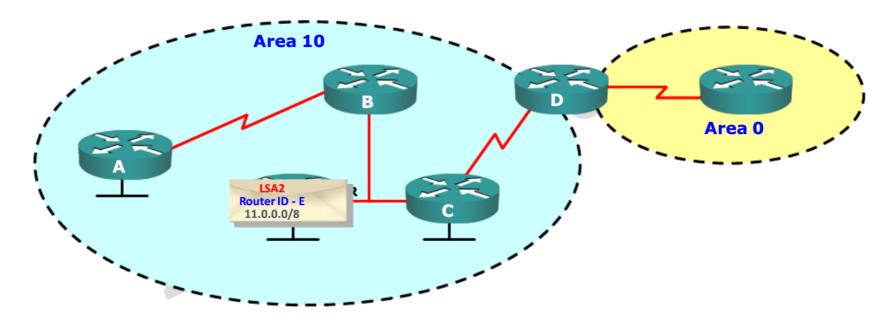
- · One Network (type 2) LSA for each transit broadcast or NBMA network in an area
  - ..att Includes Network ID, subnet mask and list of attached routers on that transit link
- Advertised by the DR of the transit network
- · Floods within its area only; does not cross ABR





### **LSA Type 2: Network LSA**







### **LSA Type 3: Summary LSA**



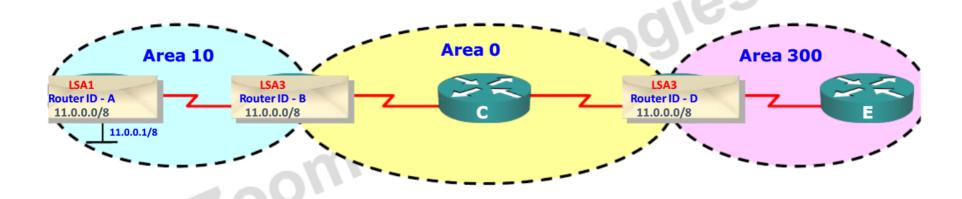
- Type 3 LSAs are used to flood network information to areas outside the originating area (inter-area)
  - contains network ID and subnet mask
- Advertised by the ABR of originating area
- Regenerated by subsequent ABRs to flood throughout the autonomous system.
- By default, routes are not summarized and there is one type 3 LSA for every subnet





### **LSA Type 3: Summary LSA**







### **LSA Type 4: ASBR Summary LSA**



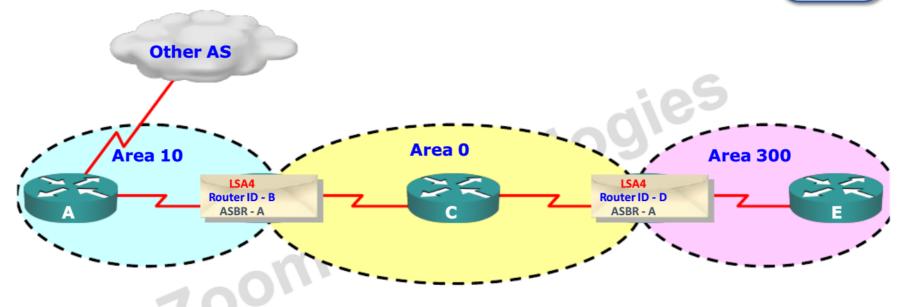
- · ASBR Summary (type 4) LSAs are used to advertise Router ID of ASBR to all routers in other areas present in autonomous system
- They are generated by the ABR of the originating area
- They are regenerated by all subsequent ABRs to flood throughout the autonomous system Type 4 LSAs contain only the router ID of the ASBR





### **LSA Type 4: Summary LSA**







### **LSA Type 5: External LSA**



- External (type 5) LSAs are used to advertise networks learned from other autonomous systems
- Type 5 LSAs are advertised and owned by the originating ASBR
- Type 5 LSAs flood throughout the autonomous system
- The advertising router ID (ASBR) is unchanged throughout the autonomous system
- Type 4 LSA is needed to identify ASBR

Zoom

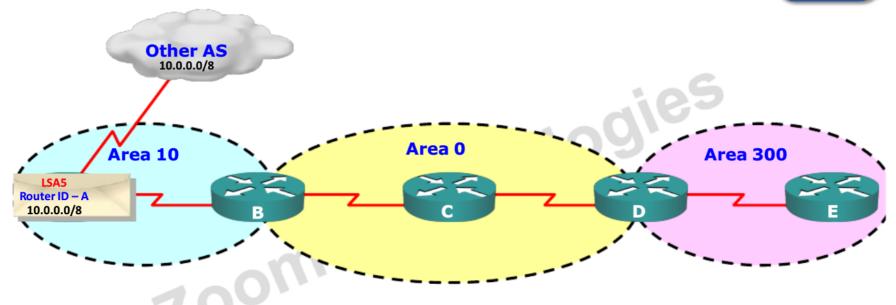
By default, routes are not summarized by ASBR





### LSA Type 5: External LSA







### **Types of Routes**



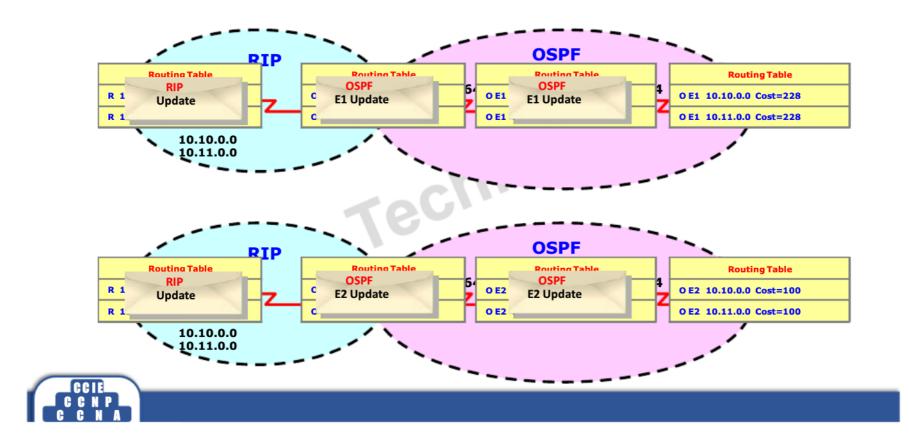
Router Designator		Description
О	LSA 1	Networks from within the area of the router
O IA	OSPF interarea (summary LSA)	Networks from outside the area of the router, but within the OSPF autonomous system
0 E1	E1 external routes	Networks outside of the autonomous system of
O E2	E2 external routes	the router





### **Cost for External Updates**





### **Default Routes in OSPF**



- OSPF can send Default Route in update
- A default route is sent as an external LSA type (O\*E2)
- ogies • Static Default Route needs to be defined in Originating router

Router(config)#ip route 0.0.0.0 0.0.0.0 <Exit Int/next-hop-IP>

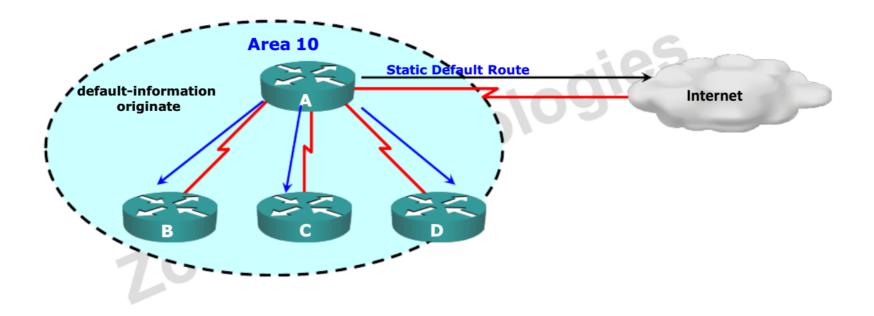
Router(config-router)# default-information originate





### **Default Routes in OSPF**









### **Defining Virtual Links**

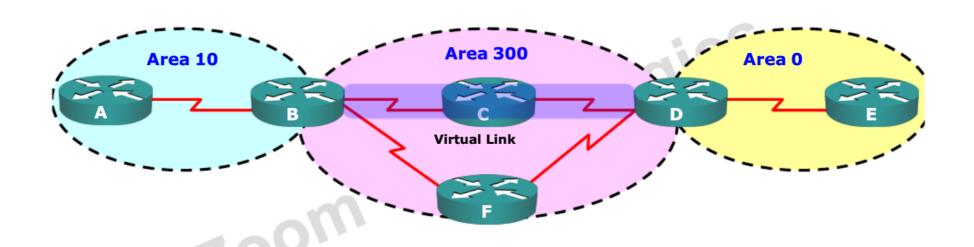


- · Virtual links are used to connect a discontiguous area to area 0
- A logical connection is built between routers
- ...ections • Virtual links are recommended for backup or temporary connections



### **Virtual Links**









### **Configuring Virtual Links**



**Configuring Virtual Link** 







# Stub and Totally Stubby Area Rules



- · There should not be an ASBR in the area
- The area should not be Area 0
- · No virtual links must pass through the area
- Zoom Technologies There should be a single ABR (recommended)



### **Using Stub Areas**



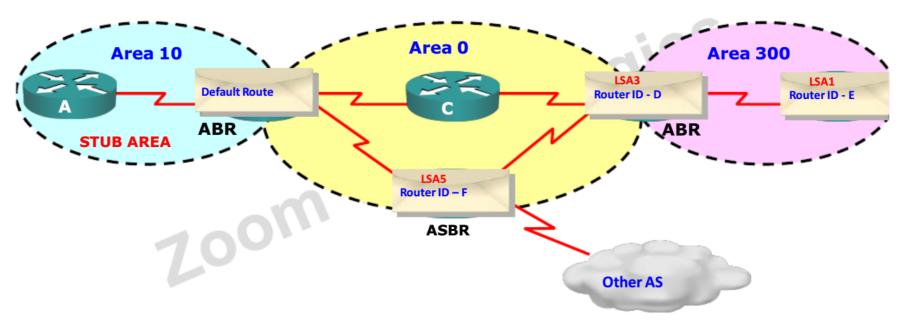
- External LSAs are stopped
- Zoom Technologies Default route is advertised into stub area by the ABR
- All routers in stub area must be configured as stub





### **Stub Area**







# **Stub Area Configuration**



Configuring Stub command on all router in the area

Router(config-router)# area <area-id> stub





# **Using Totally Stubby Areas**



- External LSAs are stopped
- Summary LSAs are stopped

- All routers in stub area must be configured as stub

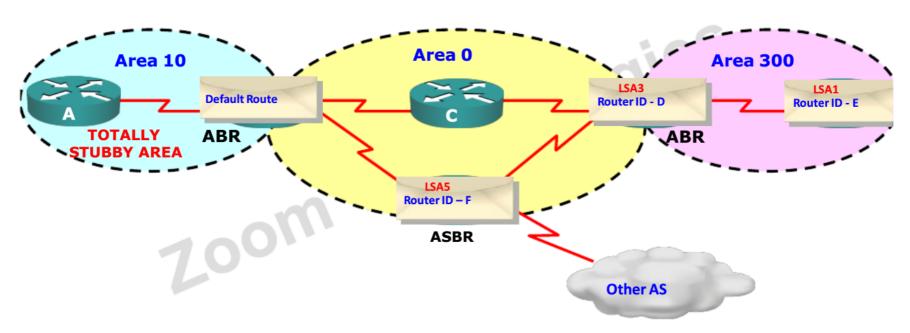
   ABR of stub area must be configured as totally stubby

   This is a Cisco proprietary feature



# **Totally Stubby Area**









# **Totally Stubby Configuration**



### **Configuring all routers of Totally Stubby Area**

Router(config-router)# area <area-id> stub ·huoloa

**Configuring Area Border Router of Totally Stubby Area** 

Router(config-router)# area <area-id> stub no-summary



### **Not-So-Stubby Areas**



- NSSA breaks stub area rules
- ASBR is allowed in NSSA

- ABR does not send default route into NSSA by default

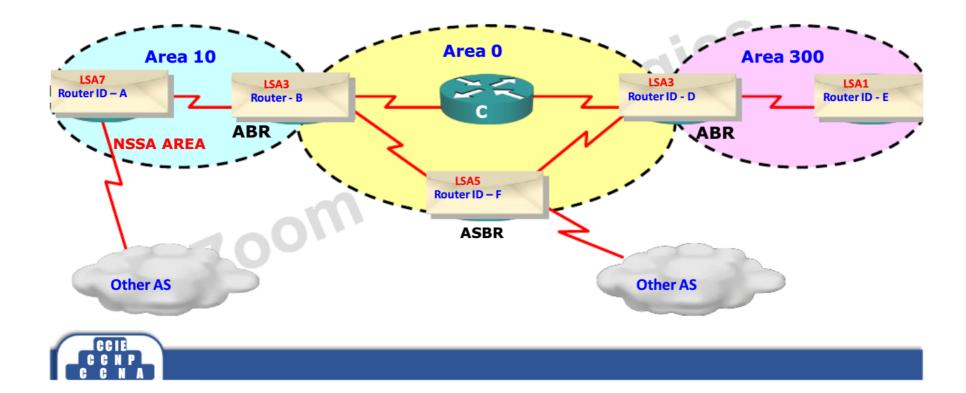
  NSSA is an RFC addendum





### **NSSA Area**





# **NSSA Area Configuration**



Configuring NSSA command on all router in the area

Router(config-router)# area <area-id> nssa





# **Totally Not-So-Stubby Areas**

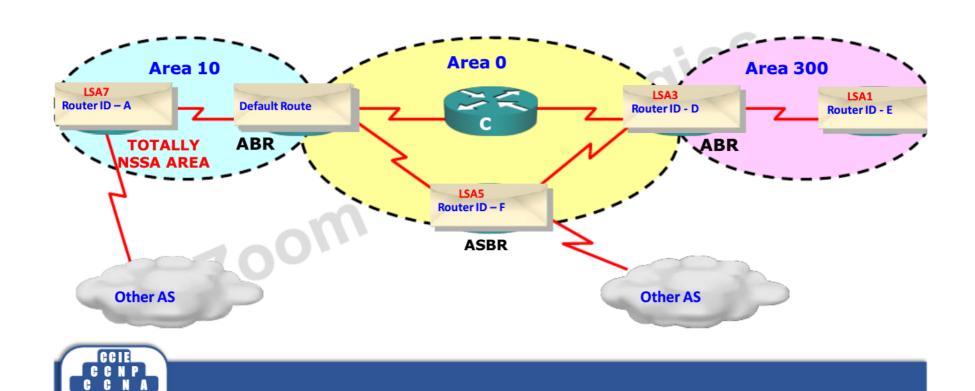


- Totally NSSA Does not accepts summary and external LSAs
- By default, Default Route is advertised by ABR of Totally NSSA



# **Totally NSSA Area**







# **Totally NSSA Area Configuration**



Configuring NSSA command on all routers in the area

Router(config-router)# area <area-id> nssa

**Configuring NSSA command on ABR router in the area** 

Router(config-router)# area <area-id> nssa no-summary

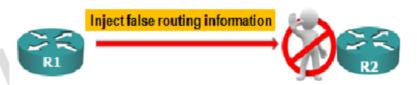


### **OSPF Authentication**



OSPF supports two types of routing protocol authentication methods

- 1) Clear Text or Plain Text
- 2) MD-5 Authentication



Routers will accept the routing information from other routers that have been configured with the same password or authentication information.





### **OSPF Authentication**



### 1) Clear Text or Plain Text

Router(conf-if)#ip ospf authentication

Router(conf-if)# ip ospf authentication-key ccnp

### 2) MD-5 Authentication

Router(conf-if)#ip ospf authentication message-digest

Router(conf-if)#ip ospf message-digest-key key-id md5 ccnp





mologies

# **Reasons for using Multiple Routing protocols**



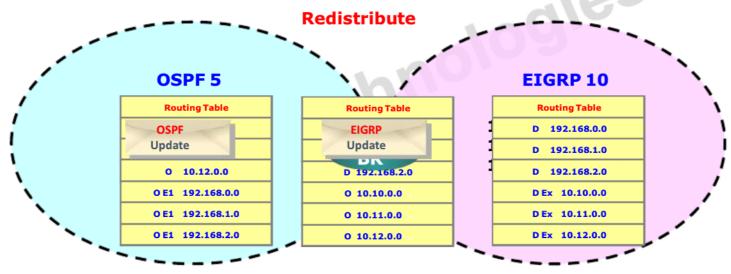
- Application-specific protocols
- Zoom Technologies Mismatch between devices (Vendors)
- Political boundaries



### Redistribution



· This process of exchanging routing information between routing protocols is called **Route Redistribution** 







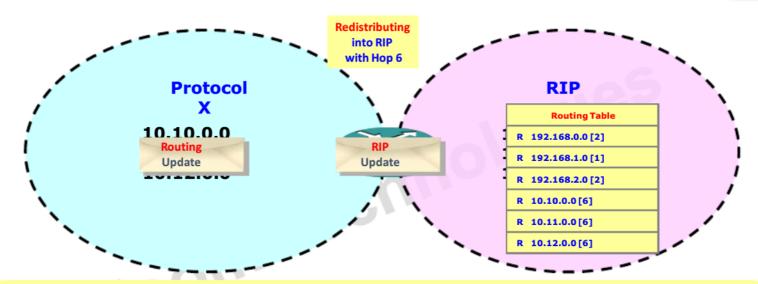


Protocols	Metric
RIP	Infinite
OSPF	20
IGRP and EIGRP	Infinite
IS – IS	0
BGP	From IGP



# **Redistributing into RIP**





**Configuring Redistribution into RIP** 

BR(config)# router rip

BR(config-router)# redistribute <protocol>

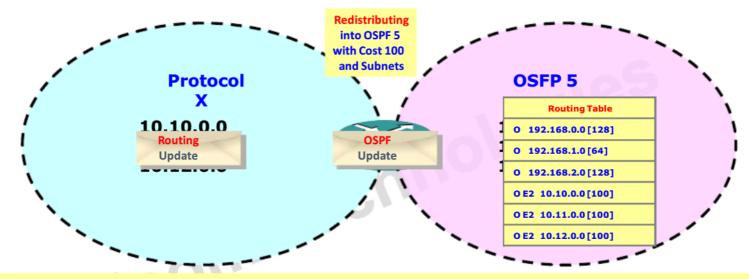
metric <value>



# **Redistributing into OSPF**



ZOOM



Configuring Redistribution into OSPF

BR(config)# router ospf 5

BR(config-router)# redistribute <protocol>

[metric <value>] [metric-type 1|2]

[subnet]



### **Redistributing into EIGRP** Redistributing into EIGRP 10 with BW 2Mbps, Delay 2000 μs, Reliblity 100% Load 50%, **Protocol** EIGRP 10 MTU 1500 10.10.0.0 D 192.168.0.0 [45002100] D 192.168.1.0 [2100150] **Update Update** D 192.168.2.0 [45002100] DEx 10.10.0.0[1200300] DEx 10.11.0.0 [1200300]

**Configuring Redistribution into EIGRP** 

BR(config)# router eigrp 10

BR(config-router)# redistribute < protocol>

metric <BW in Kbps> <delay in μs>

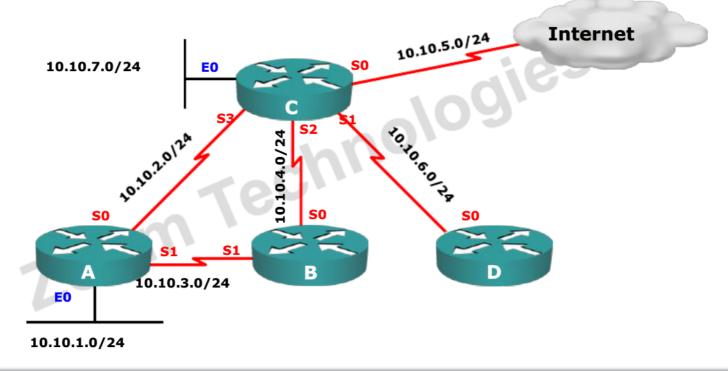
<reliability> <load> <MTU>



### **Passive Interface**



Passive Interface is the interface which will not send hello packets on the interface





### **Passive Interface Command**



**Configuring Passive Interface in routing protocol** 

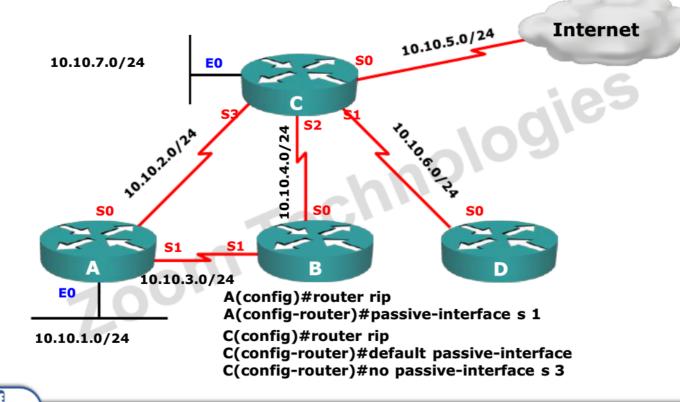
Router(config-router)# passive-interface <type> <No.>

700m



### **Passive Interface**





### **Distribute Lists**

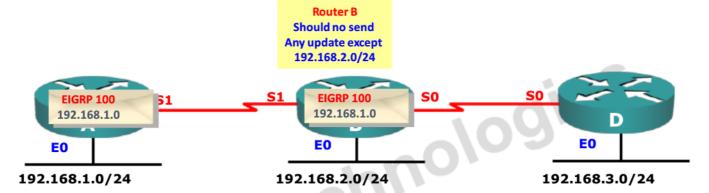


- Distribute List is a method of filtering routing updates. ..de.
- · Filtering can be inbound or outbound.
- Distribute List will be applied in router mode.



### **Distribute List**





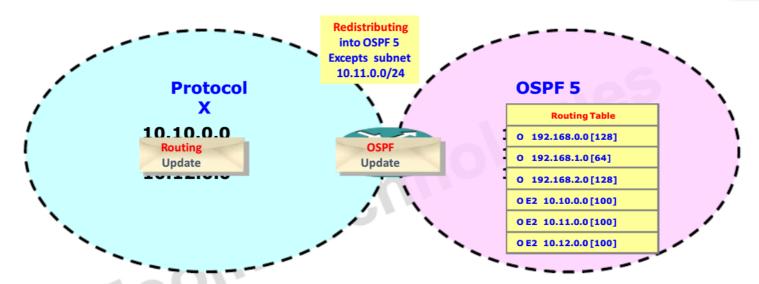
**Configuring Distribute-list on Router B** 

Router(config)# Router eigrp 100



# **Distribute List**





**Configuring Distribute-list on Router B** 

Router(config)# Router ospf 5





# **ROUTE Maps**



- Route maps work like a scripting language
- It works like a sophisticated access-list
- Top down processing
- · Once a match is found, the remaining statements are no longer processed
- Route maps are configured with sequence numbers for easy editing i.e. for adding ,removing and inserting new statements.
- · Route maps are identified by names
- Route maps will follow "IF THEN ELSE" criteria





# **ROUTE MAPS – Usage**



- · Route maps are used for
  - Zoom Technologies policy based routing
  - BGP policy
  - Redistribution
  - NAT
  - QoS



# **Configuration Of Route MAP**



**Configure Route Map** 

Router(config)# Route-map <name> permit/deny <Sequence No.>

**Defining the condition to Match** 

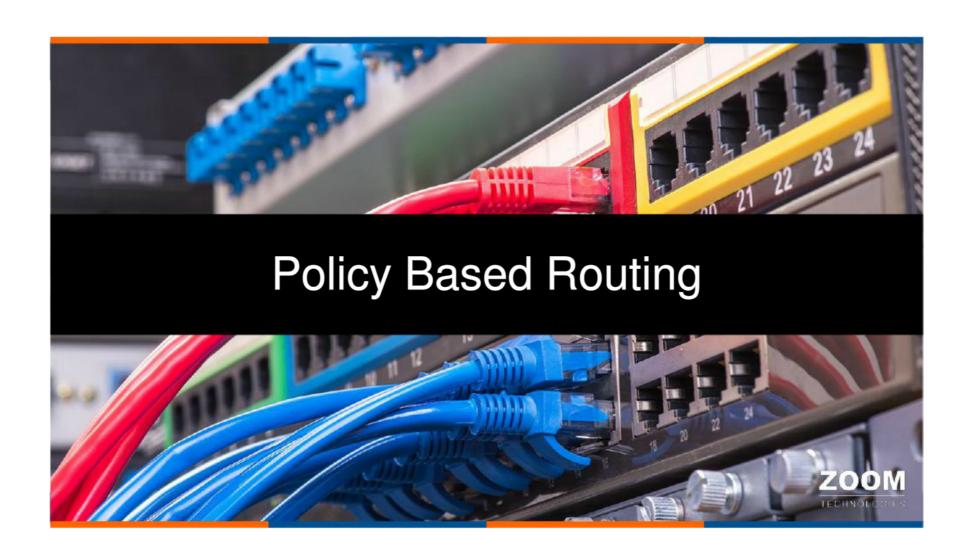
Router(config-route-map)#match <condition>

**Defining the condition to Set** 

Router(config-route-map)#set <condition>







# **POLICY BASED Routing**



- It is used for implementing a policy that causes the packet to take a different direction
- Zoom Technologies Routing table is destination based
- · PBR allows source based routing



# **POLICY BASED Routing**



- ADVANTAGES
- Zoom Technologies Different users can use different paths to reach the destination
- Load sharing



### **POLICY BASED Routing**



### **Features**

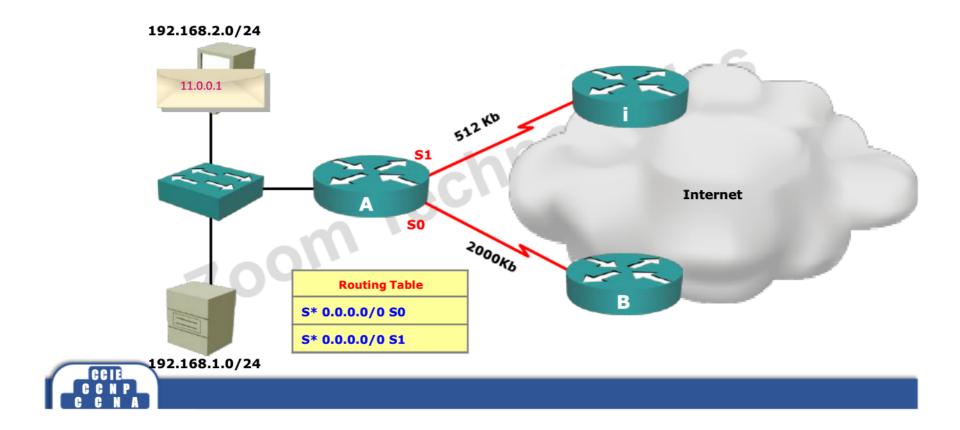
- Implemented in the incoming direction of the source interface
- If a match is found in the route map and it is permitted, the packet will be sent according to the policy
- If a match is found in the route map and it's not permitted, then it will be forwarded according to the normal routing table.
- · If there is no match th Route-map the packet will be forwarded according to routing Zoom

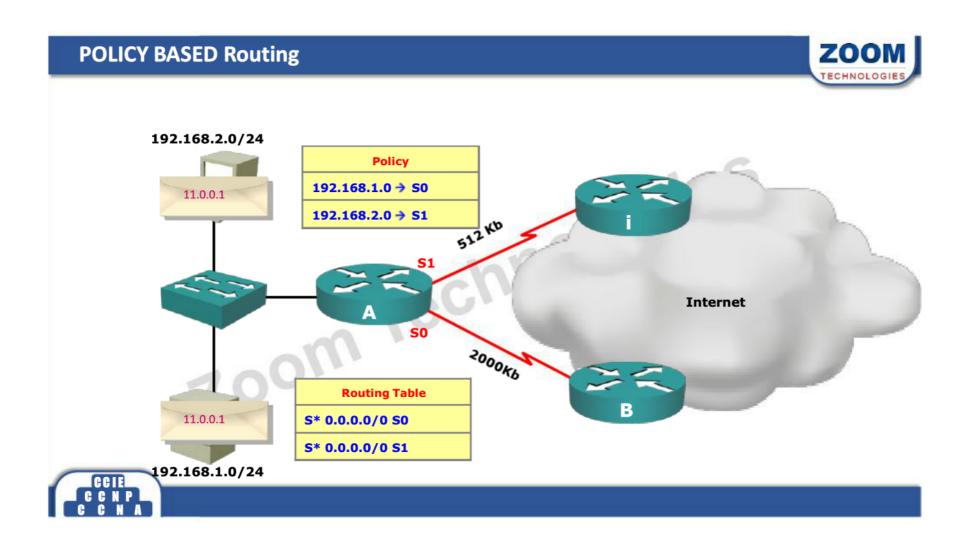




# **Before POLICY BASED ROUTING**







# **Defining Policies For PBR**



### **Configure Route Map**

Router(config)# Route-map <name> permit/deny <Sequence No.>

### **Defining the condition to Match**

Router(config-route-map)#match ip address <ACL-No.>

Or

Router(config-route-map)#match interface <type> <No.>

### **Defining the condition to Set**

Router(config-route-map)#set ip next-hop IP>

Or

Router(config-route-map)#set interface <type> <No.>



# **Implementing PBR**



### **Implementation Of PBR**

Router(config-if)# ip policy route-map <name>

7.00m Te





# With in AS IGP works ex. RIP, OSPF, EIGRP, ISIS Between AS EGP works BGP

 Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS





# IANA



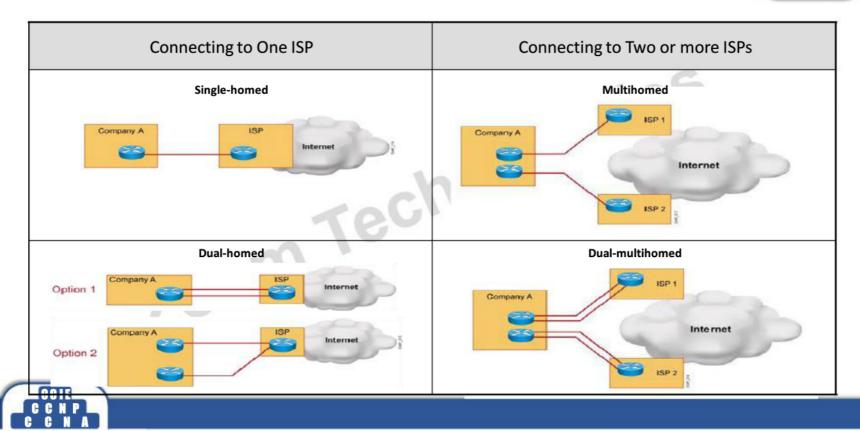
The IANA is responsible for allocating AS numbers through five Regional Internet Registries (RIRs).





# **Connection Redundancy**





### When to use BGP



- BGP is more appropriate if one of the following conditions exist
  - A.S. Is working as transit A.S. (Ex. ISP)
  - A.S is connected to multiple A.Ss
  - The traffic path for data entering or leaving the A.S. needs to manipulated



### When not to use BGP



- · BGP is not recommended if one or more following conditions exist
  - If it is a Single-homed A.S
  - · Lack of resources like memory and processing power in routers
  - Low bandwidth link between A.Ss
  - Limited understanding about BGP route filtering and path selection processes





### **BGP Features**



- Open Standard
- Advanced distance vector protocol
  - Path vector protocol
- · Classless.
  - Support FLSM, VLSM, CIDR, auto and manual summary (BGP-4)
- It is an Exterior Gateway protocol
- Designed to scale up for a huge inter-network like the Internet.
- Updates are incremental and triggered.



# **BGP Features (continued)**



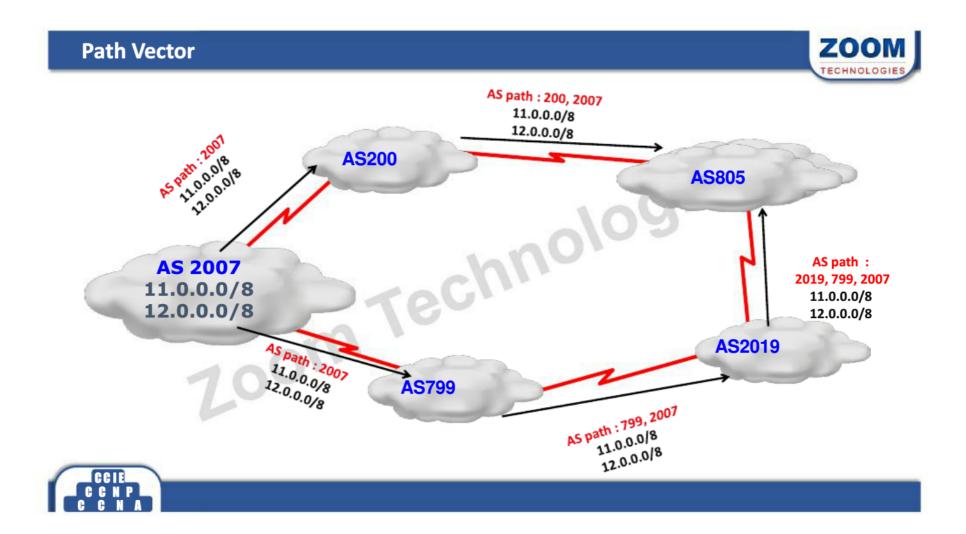
- · It sends updates to manually defined neighbors as unicast
- BGP is an application layer protocol, uses TCP for reliability, TCP port 179 logies
- Metric = Attributes
- Administrative distance
  - 20 External updates
  - 200 Internal updates

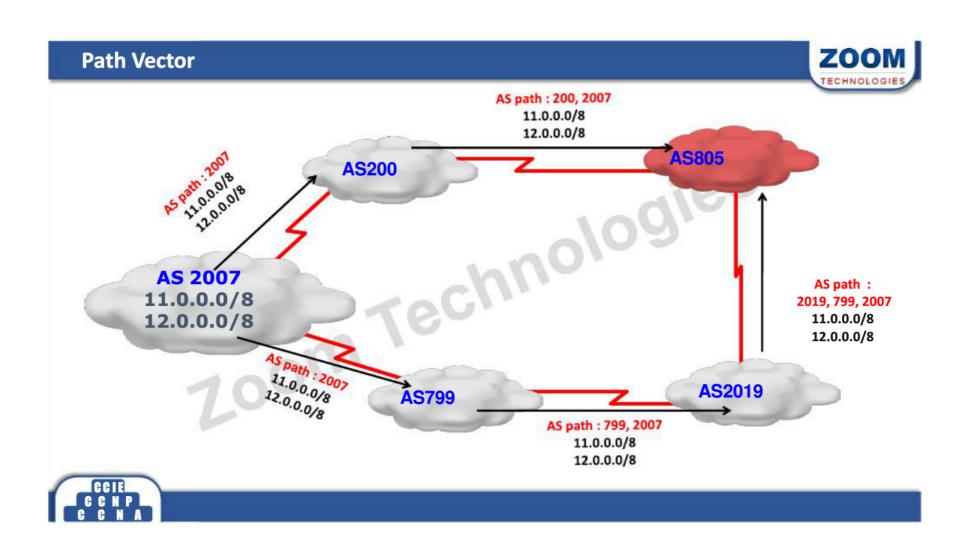
700m

BGP is not designed for load balancing. Uses only one path per network









### **Path Vector**



- IGPs announce networks and cost to reach those networks.
- BGP announces pathways and the networks that are reachable at the end of the pathway. BGP uses Attribute as Metric.
- . with les AS Path is one of the attribute of BGP. Path with less AS hop is best path.



### **BGP Databases**



- Neighbor table
  - · List of BGP neighbours
- BGP forwarding table/database
- Can contain multiple pathways to destination networks
   Database contains BGP attributes for each pathway
- IP routing table
  - List of best paths to destination networks

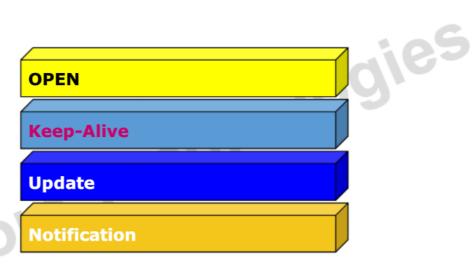
Zoom





# **BGP Message Type**







# **BGP Neighbors**



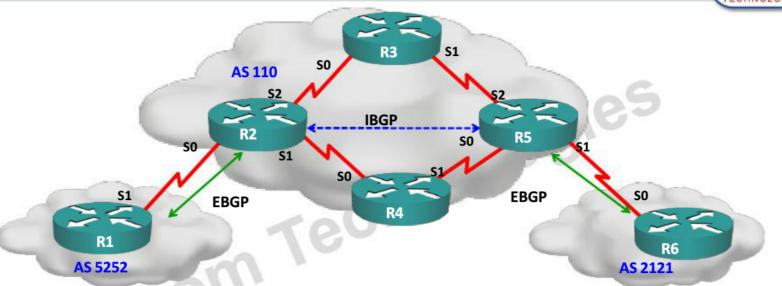
- BGP neighbors are routers forming a TCP connection for exchanging BGP updates. Also called as Zoom Technologies **BGP Peers or BGP Speakers.**
- Two type of BGP neighbor relationship.
  - IBGP (Internal BGP)
  - EBGP (External BGP)





# **BGP Neighbors**





**IBGP:** Router Forming neighbor relationship within A.S.

IBGP neighbors doesn't need to be directly connected

**EBGP:** Router Forming neighbor relationship between two different A.S.

EBGP neighbors need to be directly connected – though there may be

exceptions to this



# **BGP Configuration**



### **Configuring BGP Routing Protocol**

Router(config)# router bgp <AS no.>

### **Configuring BGP Routing Protocol**

Router(config-router)# network <network ID>

[mask <subnet mask>

- Only one instance of BGP per Router
- Same network prefix must exist in routing table
- Network may not be directly connected
- Network without subnet mask will take classful mask



# **BGP Configuration**

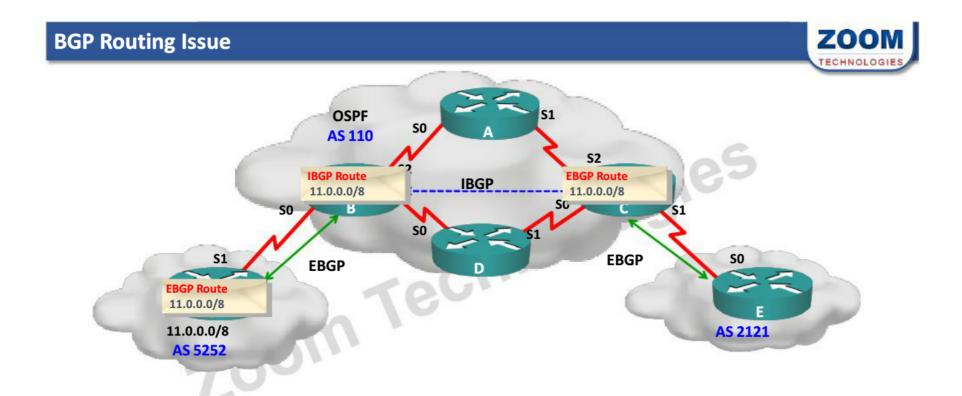


### **Configuring BGP Routing Protocol**

Router(config-router)# neighbor <IP-Address>
remote-as <AS No.>

- Router should have a route in the normal routing table to reach neighbor
- Same command for IBGP and EBGP neighbor, only the AS number will be different for an EBGP neighbor.





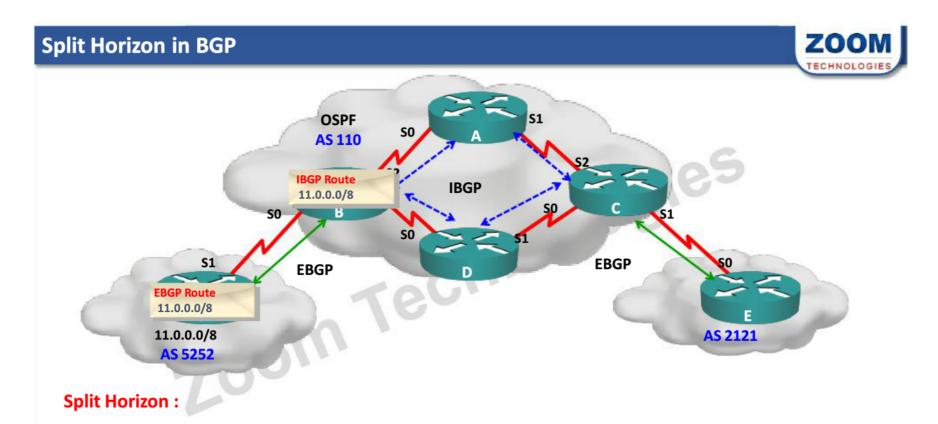




### **BGP Routing Issue** ZOON **OSPF AS 110 Routing Table IBGP** 11.0.0.0/8 S0 **Routing Table EBGP EBGP Routing Table** 11.0.0.0/8 route ? Network Int 11.0.0.0/8 S0 11.0.0.0/8 **AS 2121 AS 5252**

### **Solution:**

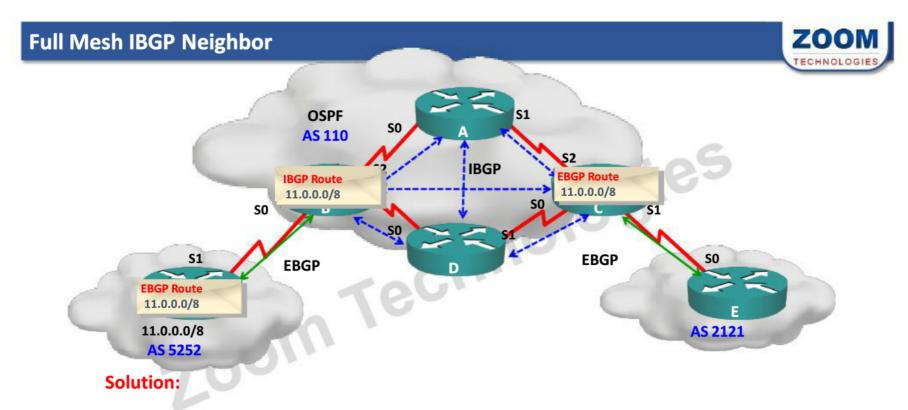
- Redistribute BGP into IGP (Not recommended)
- Run BGP on All transit routers (routers coming in path from one A.S to other)



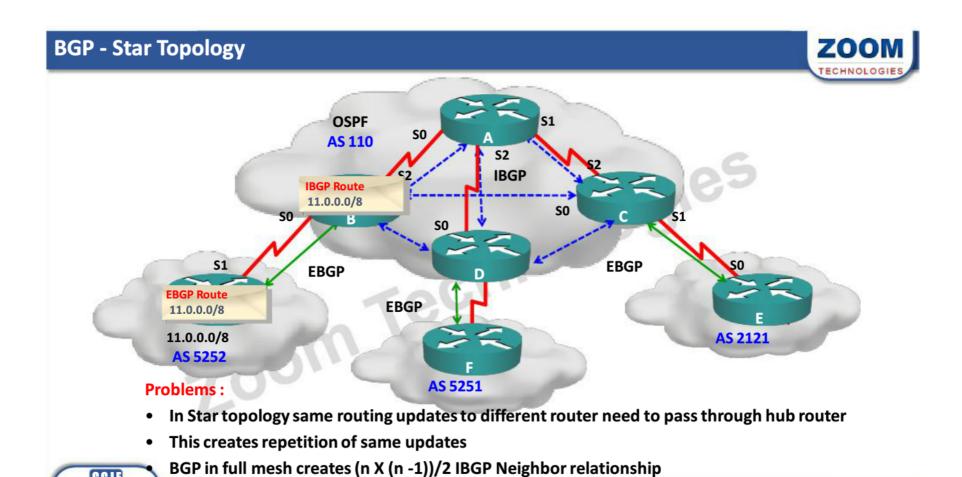
• Updates coming from IBGP neighbor cannot be forwarded to other IBGP neighbors







- Configure full mesh IBGP neighbor relationship OR
- **Use Route Reflector** CCIE



CCIE

### **Route Reflector R R Server IBGP Route** 11.0.0.0/8 **OSPF** 51 **AS 110 \$**S2 **IBGP IBGP** Route **R R Client R R Client** 11.0.0.0/8 S0 **EBGP EBGP EBGP Route R R Client EBGP** 11.0.0.0/8 AS 2121 11.0.0.0/8 **AS 5252 AS 5251**



# **Route Reflector**



- A Route Reflector is one method of disabling Split Horizon in BGP.
- By using Route Reflector, routers are divided into two roles

Zoom

- 1) Route Reflector Server
- 2) Route Reflector Client
- ogies • Route Reflector client will update server, then server will update remaining clients.



# BGP Synchronization OSPF AS 110 BGP Route 11.0.0.0/8 11.0.0.0/8 AS 5252

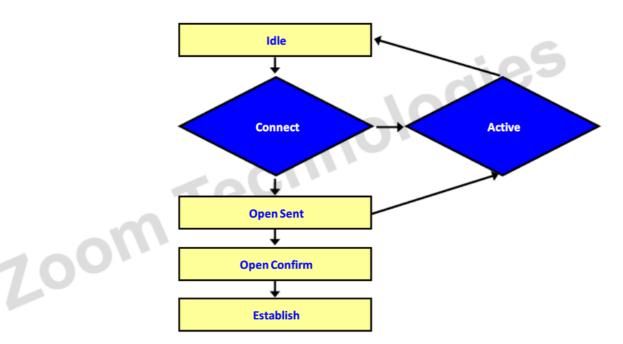
### **BGP Synchronization Rule:**

 If updates are received from IBGP neighbor, it cannot be used in routing table nor sent to other EBGP neighbor till same update comes from Interior Gateway Protocol.



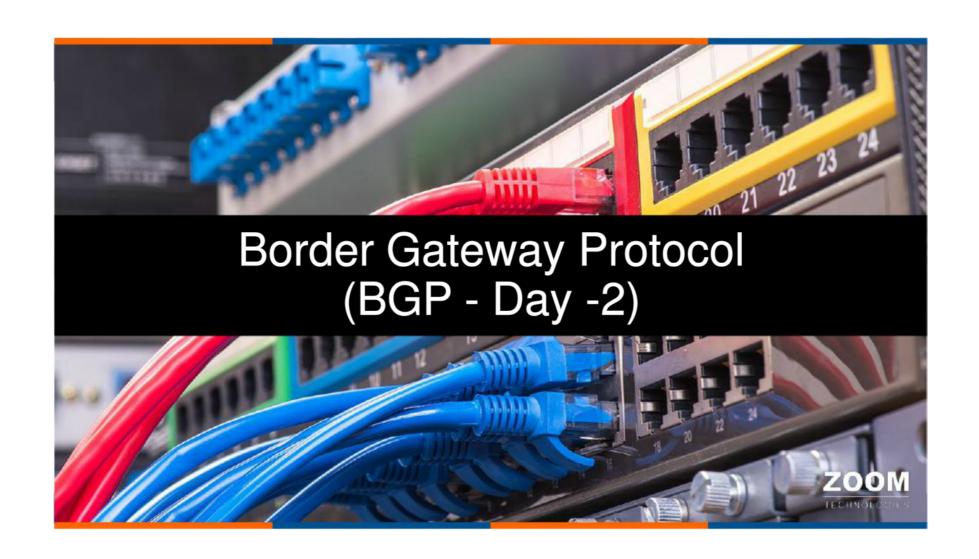
# **BGP States**

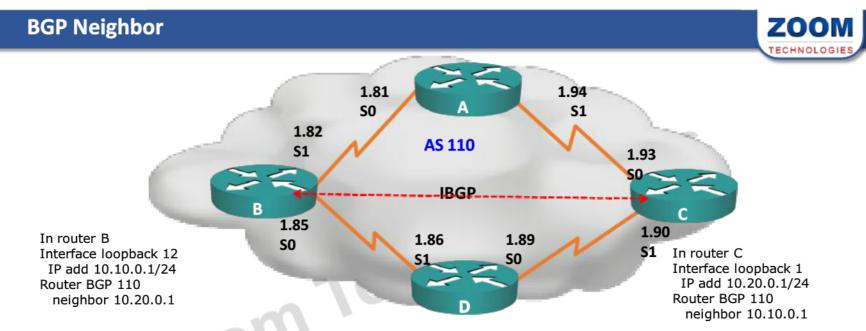












Loopback interface should be used for forming neighbor relationship. BGP messages

Destination IP = Neighbor IP

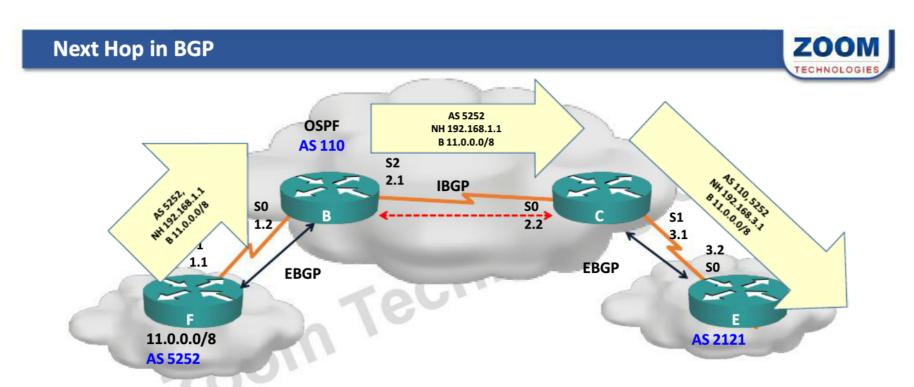
Source IP = Primary IP of Outgoing Interface

BGP check source IP in its neighbor command, if no match Message will be discarded.



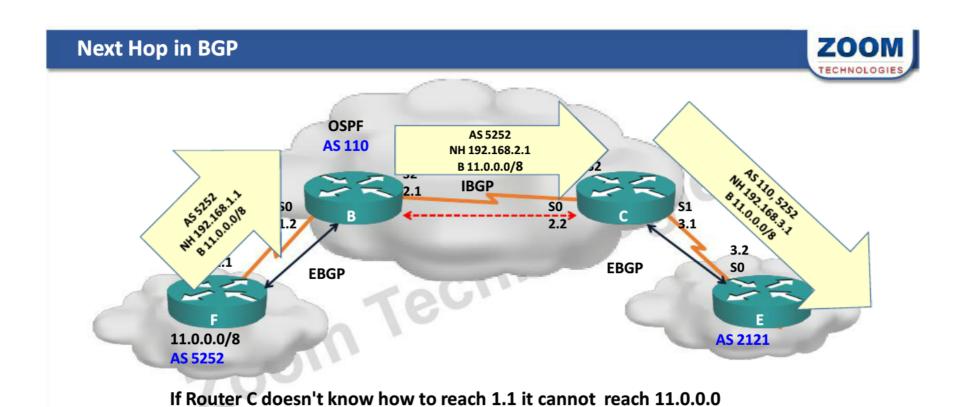
### **BGP Neighbor** ZOON 1.81 1.94 S<sub>0</sub> S1 1.82 **AS 110** S<sub>1</sub> **IBGP** 1.85 1.90 1.89 1.86 S<sub>0</sub> In router B S1 In router C Interface loopback 12 Interface loopback 1 IP add 10.10.0.1/24 IP add 10.20.0.1/24 Router BGP 110 Router BGP 110 neighbor 10.20.0.1 neighbor 10.10.0.1 On Router B B(config)#router BGP 110 B(config-router)#neighbor 10.20.0.1 remote-as 110 B(config-router)#neighbor 10.20.0.1 update-source loopback 12 B(config)#int loopback 12 B(config-if)#ip add 10.10.0.1 255.255.255.0

### **EBGP Neighbor** ZOON ECHNOLOGIE 10.0.1.1/30 10.0.1.2/30 S1 10.0.2.1/30 10.0.2.2/30 **AS 278 AS 523** On Router A A(config)#router BGP 278 A(config-router)#neighbor 10.20.0.1 remote-as 523 A(config-router)#neighbor 10.20.0.1 update-source loopback 12 A(config-router)#neighbor 10.20.0.1 ebgp-multihop 2 A(config)#int loopback 12 A(config-if)#ip add 10.10. 0.1 255.255.255.0 A(config)#ip route 10.20. 0.0 255.255.255.0 s 0 A(config)#ip route 10.20.0.0 255.255.255.0 s 1 CCIE



BGP is an AS-by-AS routing protocol, not a router-by-router routing protocol. next hop ≠ next router,

the Next-hop IP address used to reach the next AS.



network.

CCIE

## **BGP Troubleshooting**



- Clearing BGP neighbor relationship
- On modification or implementation of new policy, BGP takes time to show results. For ologies instant implementation of policies, resetting BGP peers is required.
- R#clear ip bgp \* | <neighbor IP>
- BGP resets connection and starts from Idle State.
- R#clear ip bgp \* | <neighbor IP> soft out | in
- Clears only BGP updates, TCP connection will not be reset.
- If BGP State is Idle or Active for long time.
- Check for neighbor command in both routers.
- Check whether a route exists in routing table to reach neighbor.



#### **BGP Summarization**



BGP Supports auto and manual summary.

700m

- Manual summary can be done at any point in network.
  - Summary can carry network belonging to multiple A.S.

R(config-Router)#aggregate-address < network > < mask > [summary-only]





#### **BGP Authentication**



- BGP supports MD-5 authentication.
- Configure a "key" (password); router generates a message digest, or hash, of the key and the message.
- Message digest is sent; key is not sent.

700m

Router(config-router)# neighbor <neighbor IP address> password <string>



#### **BGP Metric**



- BGP metrics are called Attributes or Rich Metrics.
- BGP attribute types:
- Well Known
  - Recognized by all the vendors.
- Optional
- chnologies May not be recognized by every vendor
- Mandatory
  - Must be present in all updates.
- Discretionary
  - May be present or not in updates
- Transitive
  - Must be sent to other neighbors.
- Non transitive
  - Only for that router. Should not be passed to neighbors.
- Partial
  - Proprietary





#### **BGP Attributes**



- Some BGP Attributes :
- AS Path
- Next hop
- Origin
- Local preference
- Zoom Technologies Multi Exit Discriminator
- Weight



#### **AS Path**



- AS Path: List of AS through which updates has traversed.
- Path with shortest AS path list is more desirable.
- AS Path is a well known, mandatory and transitive attribute.

Technologies AS path: 2007 AS path: 200, 2007 11.0.0.0/8 11.0.0.0/8 12.0.0.0/8 12.0.0.0/8 **AS 2007 AS200** 11.0.0.0/8 **AS2003** 12.0.0.0/8

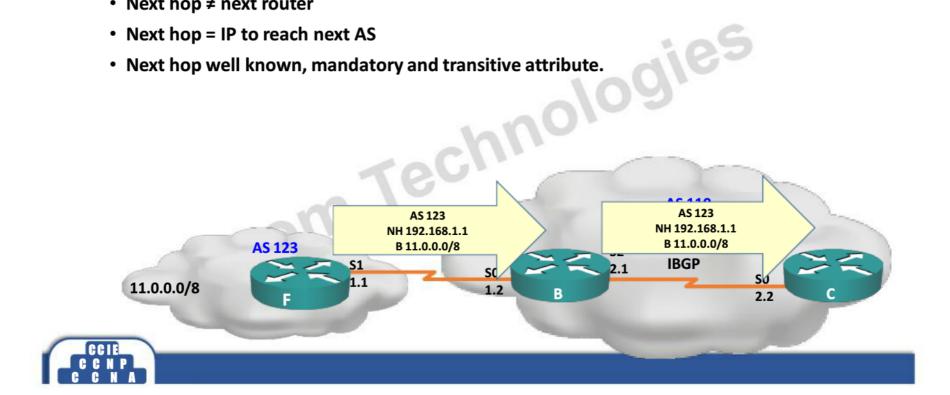




#### **Next Hop**



- BGP is AS by AS routing Protocol
- Next hop ≠ next router
- Next hop = IP to reach next AS
- Next hop well known, mandatory and transitive attribute.



## Origin



Origin informs all ASs in Internetwork how network got introduced into BGP.

mologies

- IGP (i)
  - network command
- EGP (e)
  - Redistributed from EGP
- Incomplete (?)
  - Redistributed from IGP or static
- · The origin attribute is well-known, mandatory, and transitive.
- "I" is better then "e" and "e" is better then "?"





#### **Local Preference**

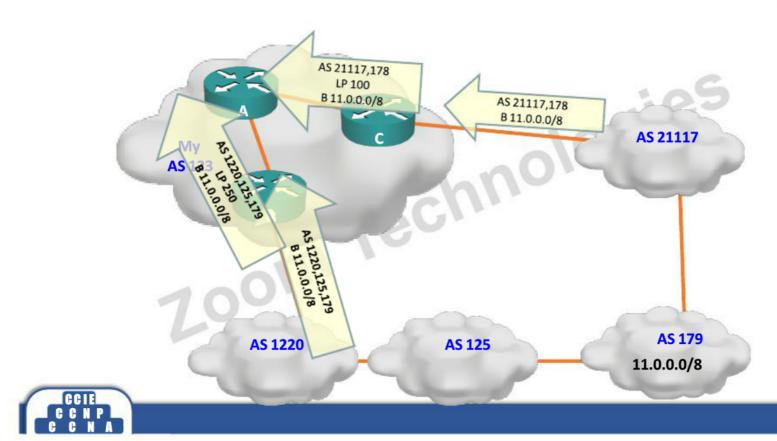


- Local preference defines how data traffic should exit from an AS.
- Default value is 100
- Path with highest preference value is more desirable.
- It is advertised only to IBGP neighbor within an AS.
- Local preference is Well known, discretionary and transitive only to IBGP neighbor.



#### **Local Preference**







# **Local Preference** 11.0.0.1 **LP 100 AS 21117** My **AS 123** rechno LP 250 **AS 179 AS 1220 AS 125** 11.0.0.0/8

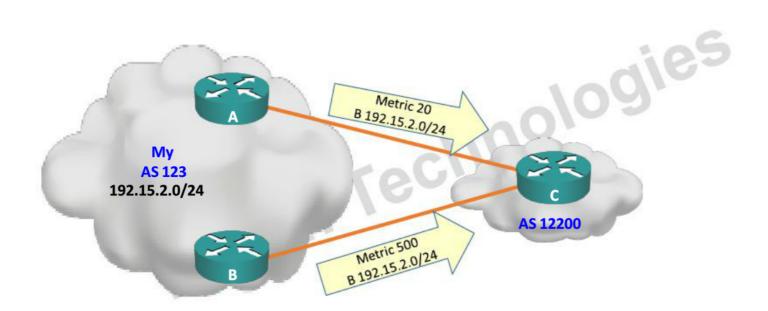
#### **MED**



- MED define how the data traffic should enter an AS.
- Default is value 0.
- · Path with less MED is more desirable.
- Zoom Technologies MED is used to advertised to EBGP neighbor only.
- MED is optional and non transitive



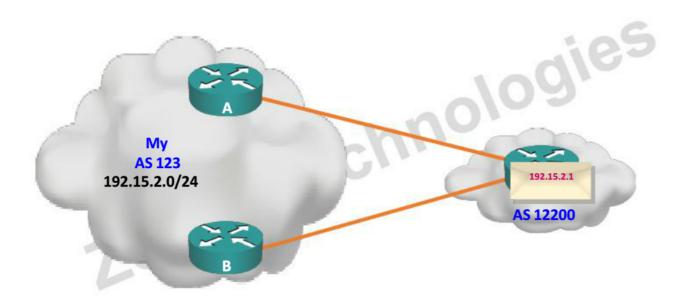






#### **MED**



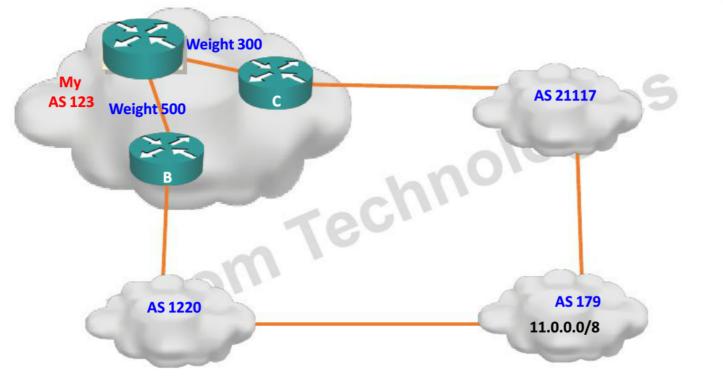






#### **WEIGHT**







#### **WEIGHT**



- · Weight is Cisco's attribute.
- Path with the highest weight is more desirable.
- Default weight is 32768 for local network and 0 for other.
- . advertisec · Weight is configured locally to each router, it is not advertised to any neighbor.
- · Weight is partial attribute.





#### **BGP Path Selection Processes**



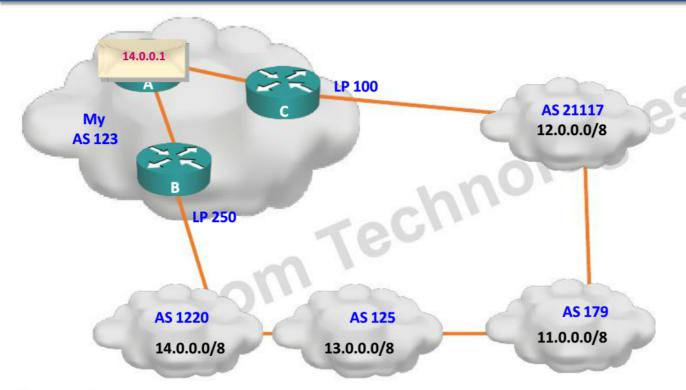
BGP Consider only (synchronized), no AS loops and a valid next hop route for path selection processes: gies

- Prefer highest weight (local to router)
- Prefer highest local preference (global within AS)
- Prefer route originated by the local router (next hop = 0.0.0.0)
- Prefer shortest AS path
- Prefer lowest origin code (IGP < EGP < incomplete)</li>
- Prefer lowest MED (from other AS)
- Prefer a path from EBGP neighbor over IBGP neighbor
- Prefer the path through the closest IGP neighbor
- Prefer oldest route for EBGP neighbor
- Prefer the path with the lowest neighbor BGP router ID



#### **Route Map for BGP policy**



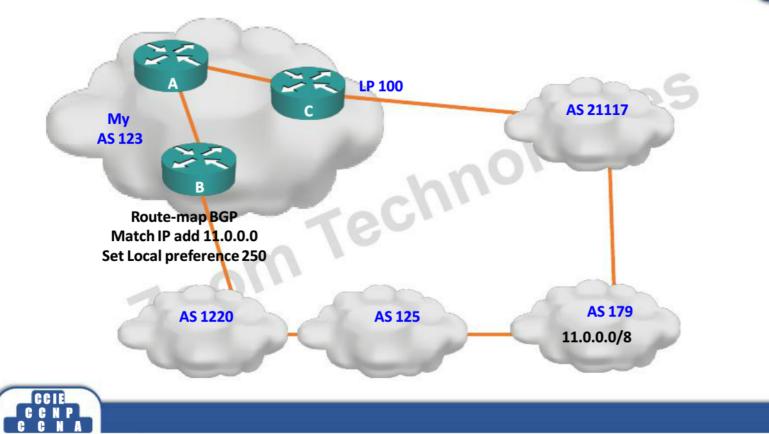






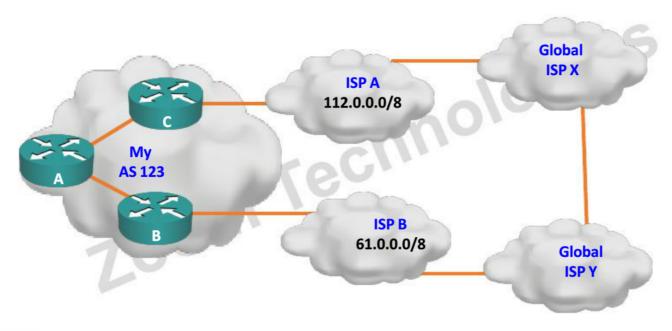
# **Route Map for BGP policy**





# **Multi-homing AS**











# Why Do We Need IPV6







## Why Do We Need a Larger Address Space?



- Internet population has grown exponentially
- Millions of Mobile users
- Transportation
- Consumer devices
- 'echnologies • No. of Websites - again exponential growth



#### **IPV4 vs IPV6**



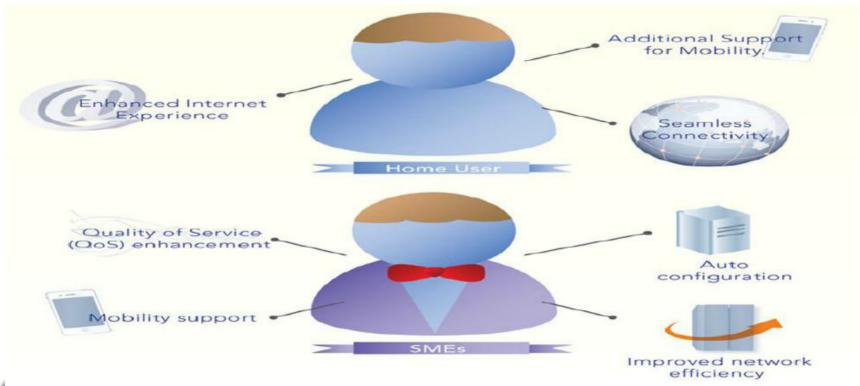
Features	IPv4	IPv6
Notation	Dotted Decimal Notation Example: 10.0.1.100	Hexadecimal Notation with Colon Example: 2001:03BB:B5A1:52FF: FEA5:4564:0112:1202
Address Size	32-bits	128-bits
Number of	2 <sup>32</sup> =	2128 =
Address	4,294,967,296 Addresses	340,282,366,920,938,463,463,374,607,431,768, 211,459 Addresses
Packet Broadcast	- Support broadcasting	- No broadcasting, IPv6 using multicast.





## **IPv6 Advantages**







#### **IPv4 vs IPv6**









## **IPv6 Address Representation**



- IPv6 Format : x:x:x:x:x:x:x:x
  - · where x is 16 bits Hexadecimal
- Leading zeros in a x field are optional
- Successive x Fields of 0 can be represented as :: but only once
   Eg. 2031:0000:0000:013f:0000:0000:0001



## **IPv4 and IPv6 Header Comparison**



#### **IPv4** Header

- 1	dentifi	cation	Flags	Fragment Offset
Time to	Live	Protocol	Heade	er Checksum
		Source Ad	dress	
		Destination	Address	3
Options				Padding

- Fields not kept in IPv6

Name and position changed in IPv6

- New field in IPv6

#### **IPv6** Header







## **IPv6 Address Type**



- Unicast
- Multicast
- Anycast

# Zoom Technologies



#### **Unicast**



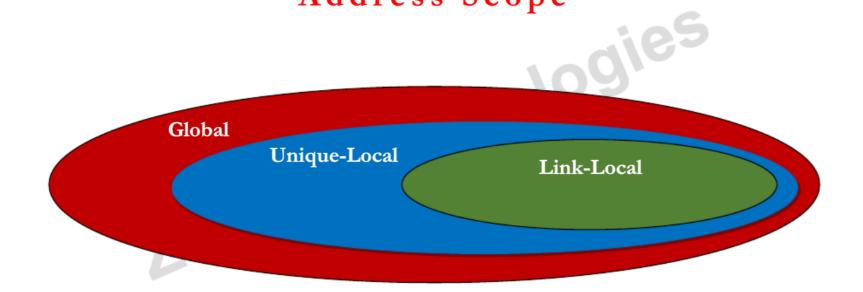
- There are three type of unicast address
  - Zoom Technologies Global Unicast
  - Unique Local
  - Link-Local







# Address Scope





#### **Global Unicast**



- Allows computers to communicate on the internet.
- The Internet Assigned Numbers Authority (IANA )delegates the current global address's prefix as 2000::/3.





## **Link Local**



- Enables communication within local link (local physical network) only.
- Equivalent to Automatic Private IP Addressing (APIPA)
- The first 10 bits of link-local IP address is set to 1111111010, which is equals to FE80 when it is converted to hexadecimal.
- A link-local IP address is always begins with FE80.



#### **Unique Local**



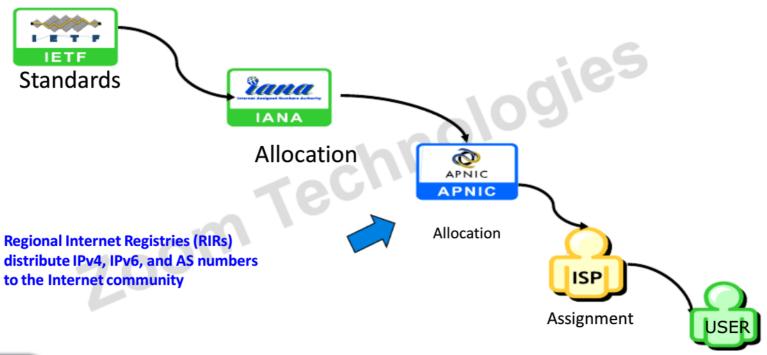
- Equivalent to private IPv4 addresses
- · Packets are routed within an organization, and not outside it on the public internet.
- In IPv4, these addresses are 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.
- IPv6's site-local addresses have set the first 10 bits to 1111111011, which equals to FC00.





#### Where do IP addresses come from?

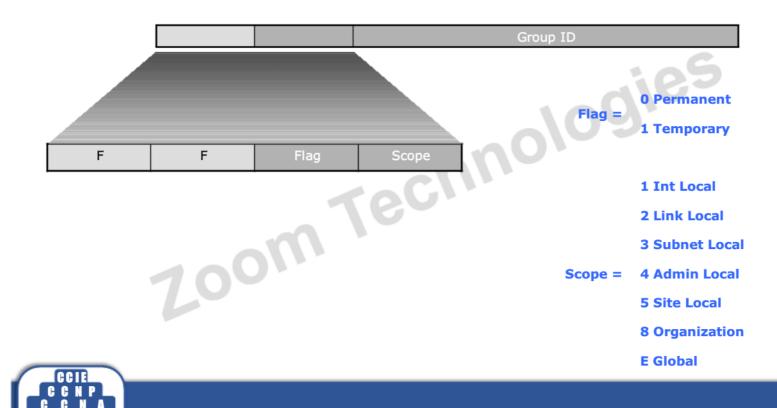






## Multicasting

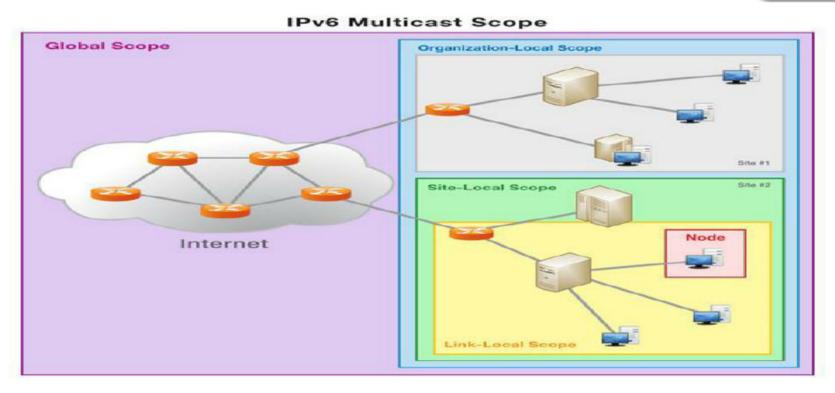






# **Multicast Scope**



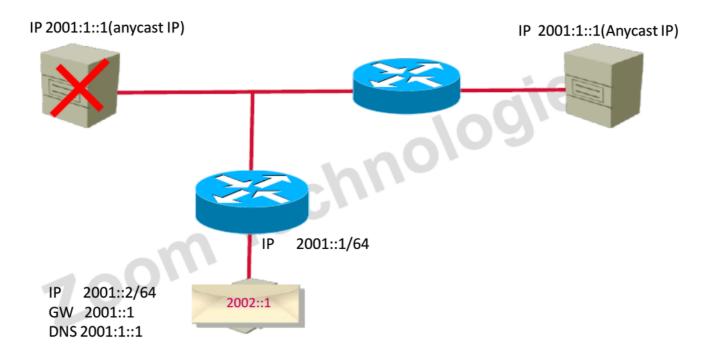






#### **Anycast**







#### **Anycast**



- One to nearest one
- Two or more devices share same anycast IP
- Zoom Technologies Nearest one will be decided by router by its routing protocol
- Anycast should give same type of service
- Anycast IP is used from Unicast range



## **Neighbor Discovery Protocol**

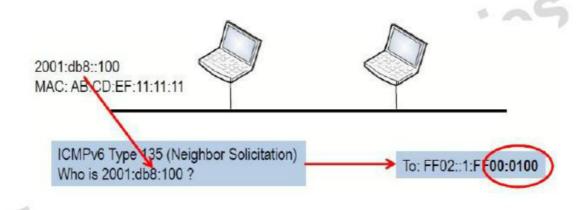


- Neighbor Discovery Protocol is Internet Protocol used in IPV6
- Zoom Technologies · NDP uses 5 different messages for the operation
- NS(Neighbor Solicitation)
- NA( Neighbor Advertisement)
- RS( Router Solicitation)
- RA(Router Advertisement)
- Redirect



DAD



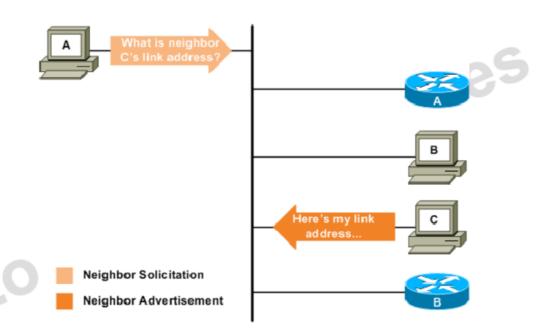






## **ARP**

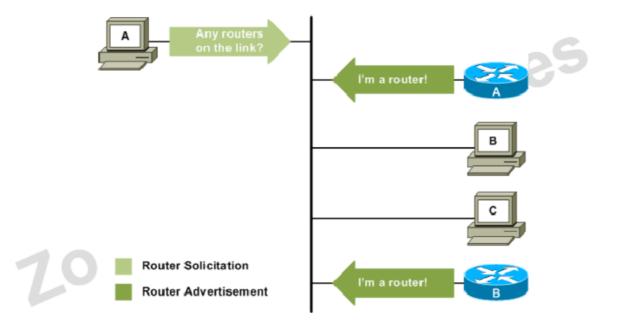






## **Router Discovery**









## **IPV6 Stateless Auto Configuration**

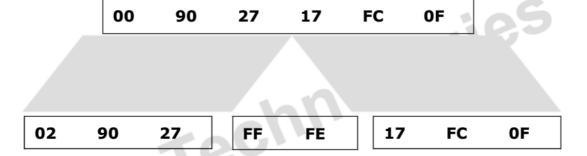


- Device will assign IP address automatically by using stateless auto configuration.
- Extended universal identifier (EUI)-64 format to do stateless auto configuration
- ing ding • This format expands the 48-bit MAC address to 64 bits by inserting "FFFE" into the middle of MAC address.
- 7th initial bit of MAC will be always "1"



#### **EUI-64 To IPv6**





0290:27FF:FE17:FC0F

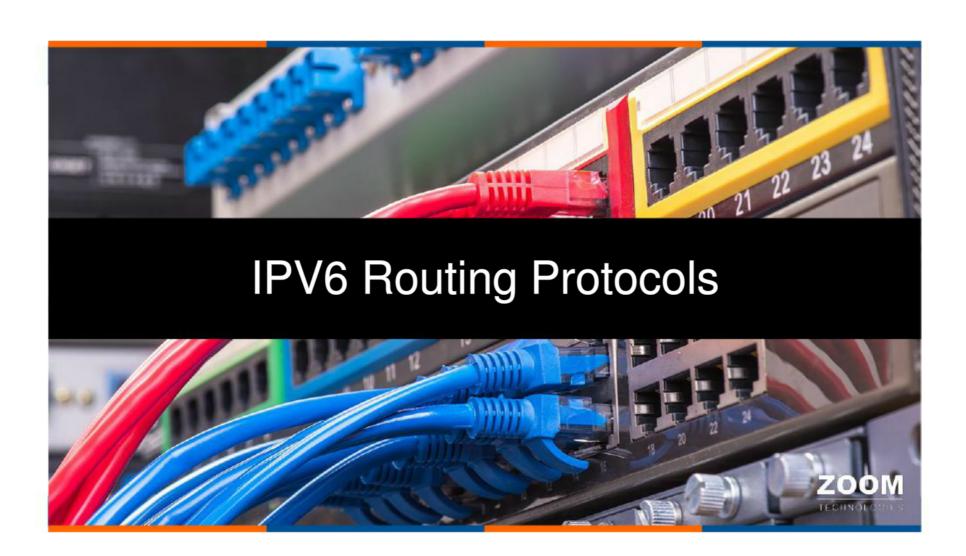






IPv6 Address	Description	
::/0	<ul> <li>All routes and used when specifying a default static route.</li> <li>It is equivalent to the IPv4 quad-zero (0.0.0.0).</li> </ul>	
::/128	<ul> <li>Unspecified address and is initially assigned to a host when it first resolves its local link address.</li> </ul>	
::1/128	<ul> <li>Loopback address of local host.</li> <li>Equivalent to 127.0.0.1 in IPv4.</li> </ul>	
FE80::/10	<ul> <li>Link-local unicast address.</li> <li>Similar to the Windows autoconfiguration IP address of 169.254.x.x.</li> </ul>	
FF00::/8	Multicast addresses.	
All other addresses	Global unicast address.	







## **IPv6 Routing Protocols**



- Static
- RIPng
- OSPFv3
- ISIS for IPv6
- Zoom Technologies • EIGRP For IPv6
- MP BGP







## **RIPng**



- RIP for IPv6
- · Based on RIPV2, with enhancements
- Distributes IPv6 prefixes
- RIPng sends updates on UDP port 521 using the multicast group FF02::9.





#### OSPFv3



- OSPF for IPv6
- Zoom Technologies Based on OSPFv2, with enhancements
- Distributes IPv6 prefixes
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2



#### **OSPFv3 / OSPFv2 Similarities**



- Link-State Protocol
- SPF or Dijkstra algorithm
- Mechanisms for neighbor discovery and adjacency formation
  Same Interface types
  LSA flooding and aging mechanism
  OSPFv3 still uses Router ID from IPv4 Address

700m





# **OSPFv3 / OSPFv2 Differences**



OSPF v2	OSPF v3
• Runs over subnet	• Runs Over a Link
One instance per link	Multiple instance per link
Clear text or MD5 authentication	Uses standard authentication
	supported by IPv6 I.E. IPSec
Router should be on the same	Router belonging to different
subnet to form neighbors.	subnet can become neighbor
Uses Primary IP of outgoing	Uses link local address as source
interface as source of updates	of updates





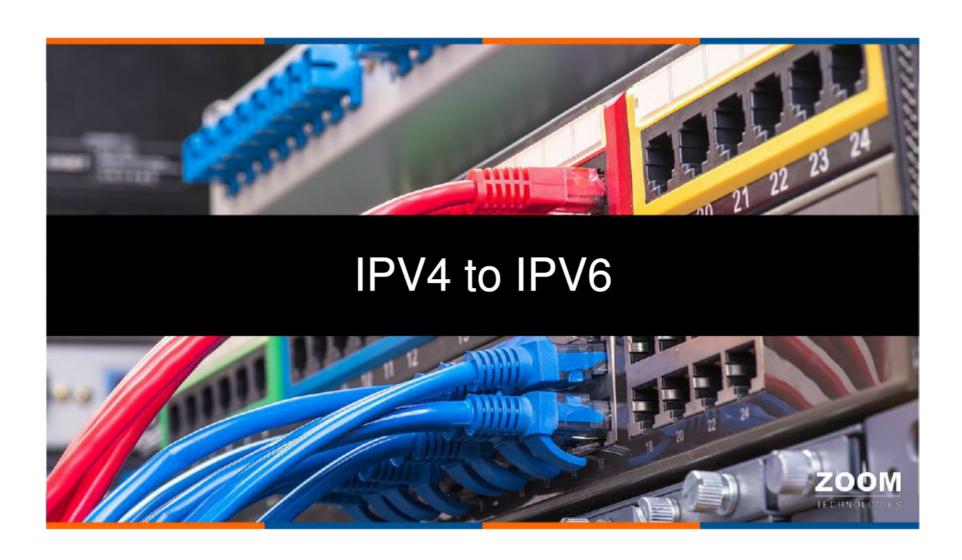


#### **EIGRPV6**



- EIGRP for IPv6
- Uses Multicast address FF02::A
- 7.00m Technologies • EIGRPV6 remains in shutdown state until no shutdown is given.
- Manually need to configure Router-ID in EIGRPV6
- EIGRPV6 also uses DUAL algoritham





#### IPv6 - IPv4 Transition



- Transition Richness
  - Zoom Technologies No Fixed day or time Due date for IPv4 to IPv6
  - Smooth transition from IPv4 to IPv6
  - Use Dual Stack or 6to4 tunnel
  - IPv4 to IPv6 host can communicate



#### **IPv4-IPv6 Transition and Co-Existence**



- · A wide range of techniques have been identified and implemented, basically falling into three categories:
  - Dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and
  - Tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions
  - vo-only da Translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices.





#### **DUAL Stack**



 The term dual stacks means that the host or router uses both IPv4 and IPv6 at the same time.



interface Ethernet0
ip address 192.168.99.1 255.255.255.0
ipv6 address 2001:410:213:1::/64 eui-64

IPv4: 192.168.99.1

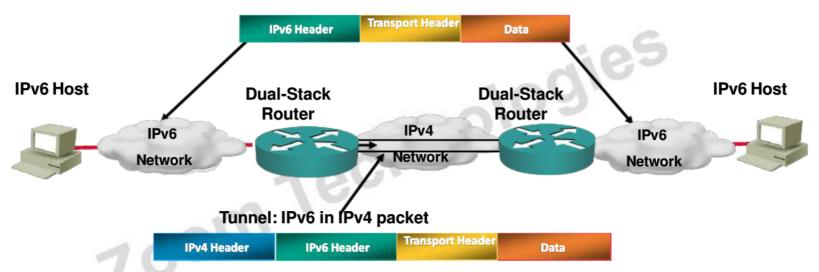
IPv6: 2001:410:213:1::/64 eui-64

- Cisco IOS is IPv6-enabled:
  - If IPv4 and IPv6 are configured on one interface, the router is dual-stacked



#### **IPv6 over IPv4 Tunnels**





- 1. Tunneling is encapsulating the IPv6 packet in the IPv4 packet
- 2. Tunneling can be used by routers and hosts





#### **NAT-PT** 2001::5 <=> 172.16.0.5 2001:3:0A00:0001 <=> 10.0.0.1 IPv4-only network **IPv6-only NAT-PT** network **IPv6 Host IPv4 Host** 2001::5 10.0.0.1 2001::5 2001:3:0A00:0001 DATA 10.0.0.1 172.16.0.5 DATA

#### **ISATAP**



- ISATAP- Intra-Site Automatic Tunnel Addressing Protocol
- ISATAP is a method of automatic 6 to 4 Tunnels.
- ISATAP is a mechanism that allows us to deploy IPv6 over existing IPv4 infrastructure.
- ISATAP connects two regions of IPv6 via a tunnel that will transit over existing IPv4 infrastructure.





## **Virtual Private Networking**





Private Network — Encryption



Virtual Private Network = Tunneling + Encryption



7126\_353



#### **VPN Services**



- oom Technologies • Services Offered by VPN are:
  - Data Security
  - Data Integrity
  - Authentication
  - Anti-Replay
  - Tunneling



## **Devices Supports VPN**









**Firewall** 

**VPN** concentrator





Servers

Cisco VPN Client v 5





## **VPN Types**

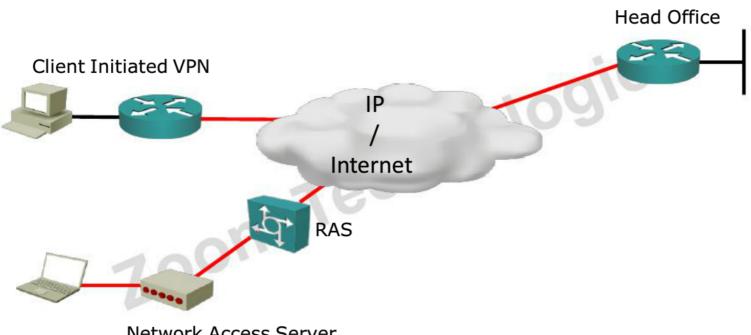


- Zoom Technologies Remote-access
  - Client-initiated
  - Network access server
- Site-to-site
  - Intranet
  - Extranet



#### **Remote Access VPN**





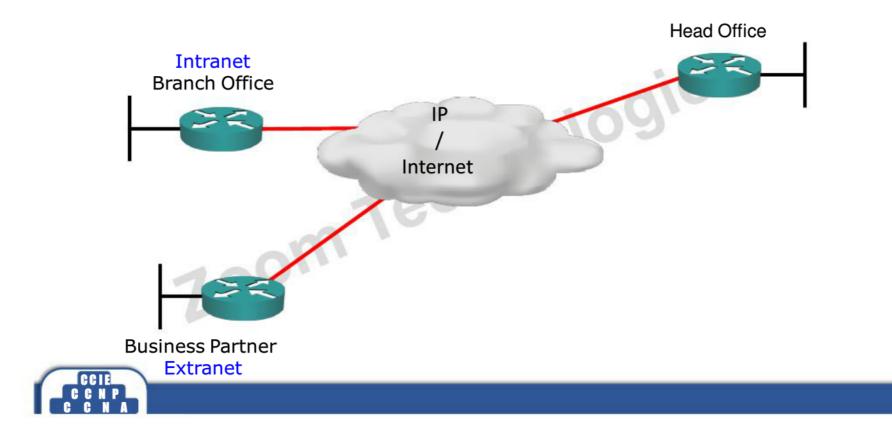
**Network Access Server** 





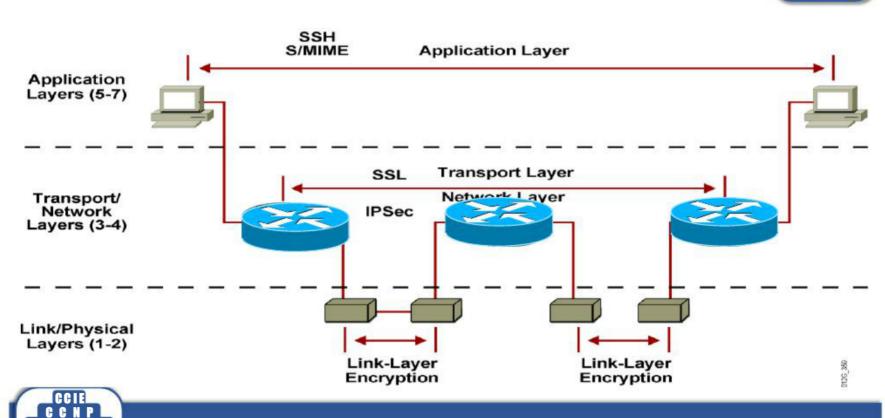
## **Site to Site**





## **Encryption at Several Layers**

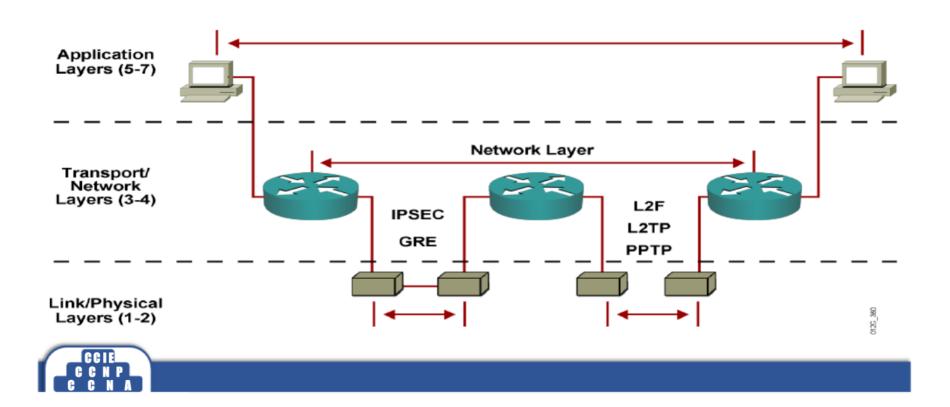


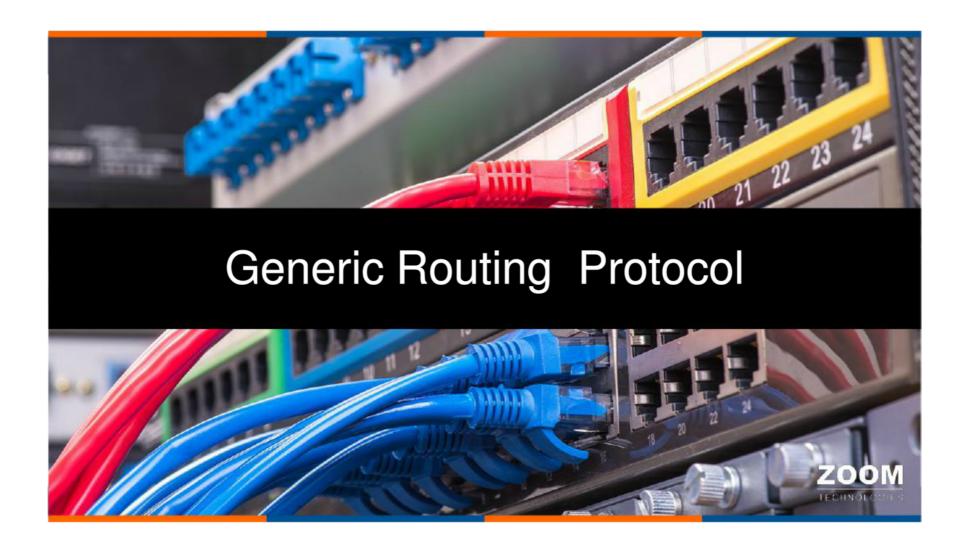




### **Tunneling Protocols**

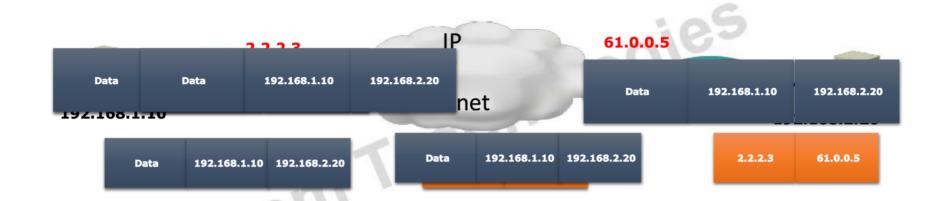






### **Generic Routing Encapsulation**











### **IPSec**



dies

- IPSec is a open standard (IETF)
- Network layer protocol
- It provides Data security and tunneling services
- It is a framework consisting of many open standards providing encryption, authentication, key exchange and data integrity.
- Scales from small to very large networks
- It can Work only for IP unicast traffic
- IPSec over GRE is used for protecting non-IP or Multicast traffic



## User Data Encryption YES IP Unicast YES IPSec Send







- IPSec modes:
  - Tunnel Mode
    - Tunnel mode creates a new additional IP header with data encryption
  - Transport mode
    - just encrypt data without adding new IP header

7.00m





### **IPSec Protocols**



- Zoom Technologies Negotiation protocol
  - IKE /ISAKMP
- Security Protocol
  - ESP
  - AH



### **IPSec Protocols**



- Encryption
  - DES
  - 3DES
  - AES
- Hash
  - MD5
  - SHA
- Authentication
  - Pre-share key
  - Username/Password
  - OTP
- Technologies • Password Protection (Diffie-Hellman for password exchange)
  - DH Group 1
  - DH Group 2





### **Internet Key Exchange**



- IKE solves the problems of manual and unsalable implementation of IPSec by automating the **Negotiation Process**  Automatic key generation, negotiation and implementation
   Negotiation of SA characteristics

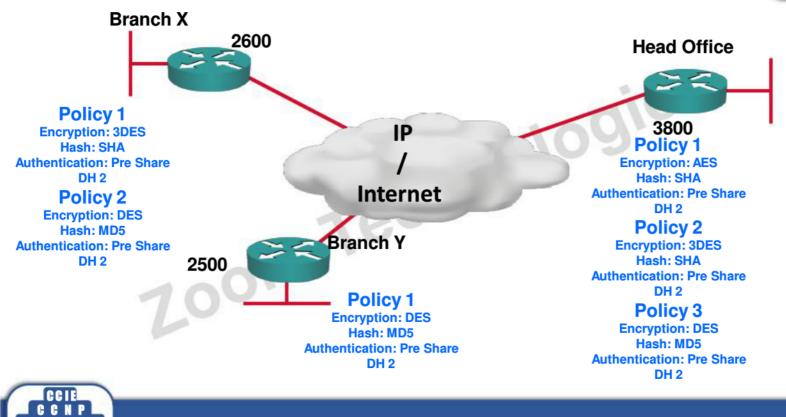
  - Manageable manual configuration

Zoom



### **IKE Negotiation**



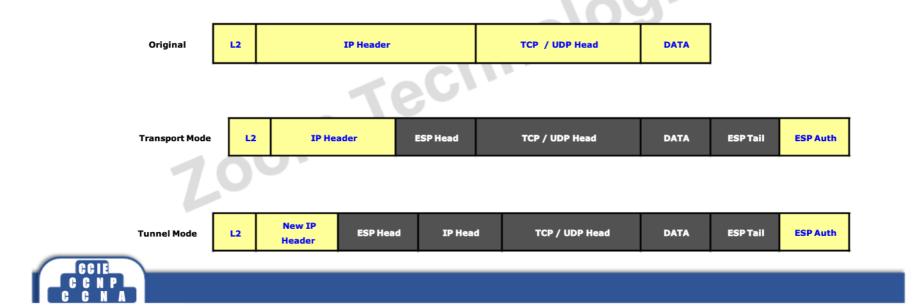




### **Encapsulating Security Payload**



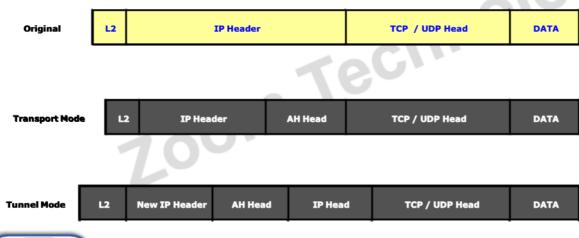
- ESP protocol ID 50
- Provides framework for encrypting, authenticating and data integrity. Optional Anti-replay



### **Authentication Header**



- AH protocol ID 51
- Provides framework for authenticating and data integrity. Optional Anti-Replay





### **DMVPN**



- DMVPN allows a vpn tunnel to dynamically created and torn down between two remote sites
- DMVPN uses NHRP and multipoint GRE to perform this operation.

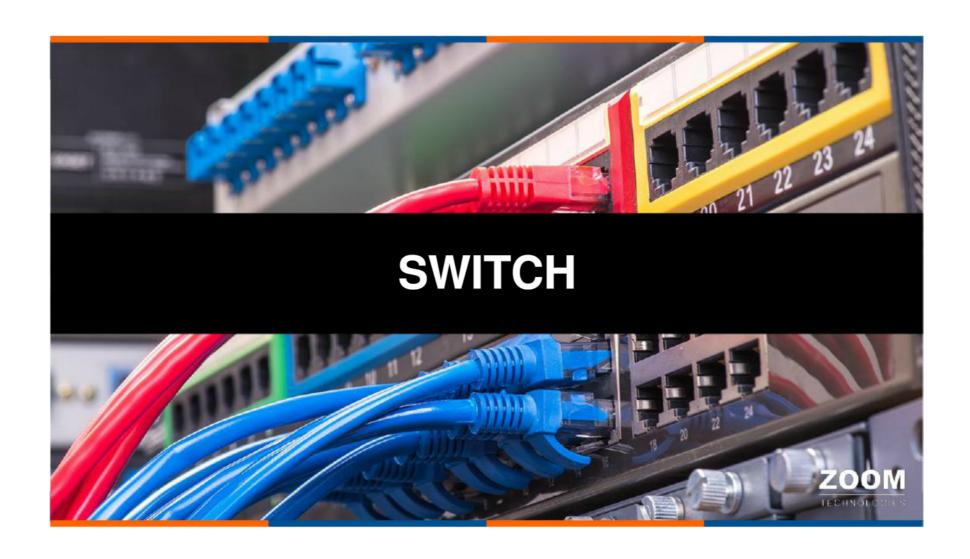








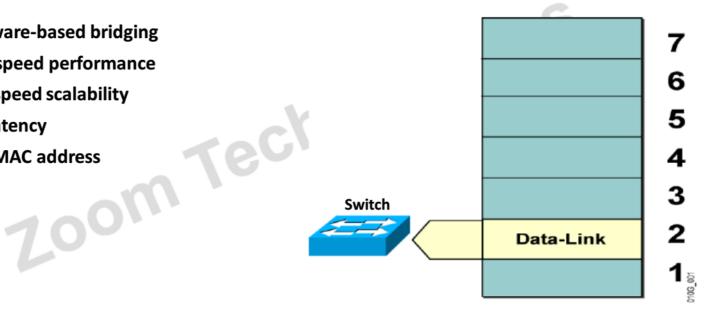
Zoom Technologies



### **Layer 2 Switching**



- Hardware-based bridging
- Wire-speed performance
- High-speed scalability
- Low latency
- Uses MAC address







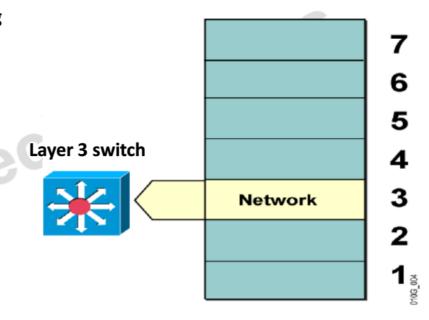
### **Layer 3 Switching**



Hardware-based packet forwarding

oom

- High-performance packet switching
- Flow accounting
- Layer 3 security
- Policy deployment





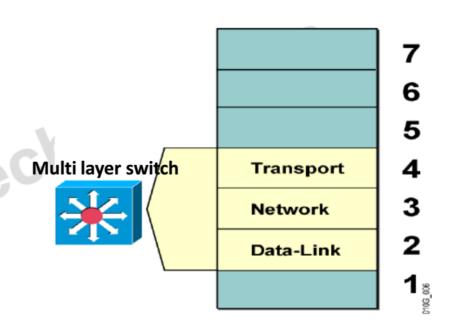
### **Multilayer Switching**



- Combines functionality of:
  - Layer 2 switching
  - Layer 3 switching
  - Layer 4 switching

room

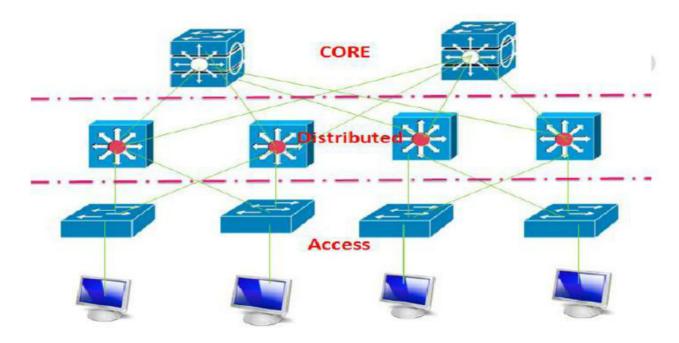
- High-speed scalability
- Low latency













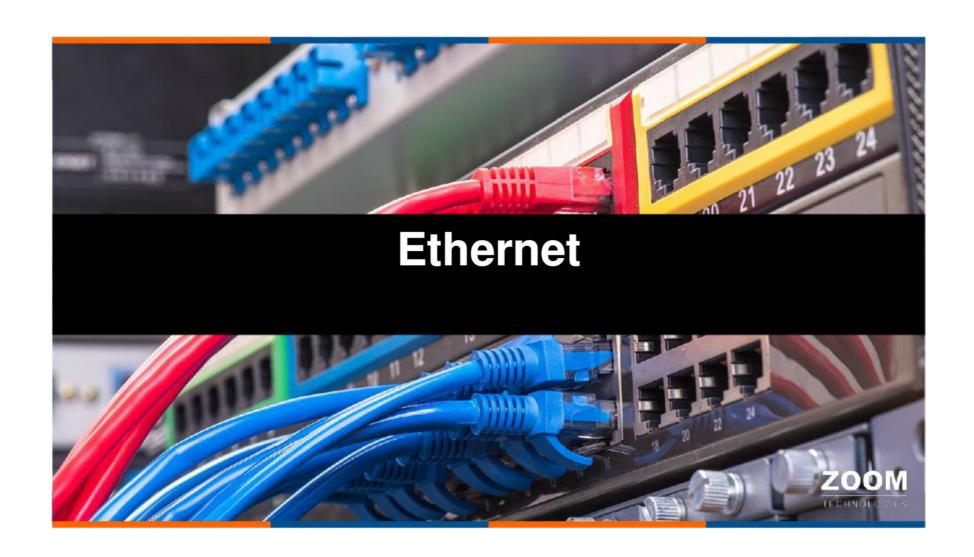
### **Types of switches**



- Access Layer:
- Access Layer switches are used to connect end devices to the network
- Access Layer Switches used to provide Layer2 ( VLAN) connectivity between users.
- Ex: 2950,2960 switches
- Distribution Layer:
- Distribution Layer switches are used to interconnect access layer switches to core layer switches.
- Distribution Layer is a Layer 3 Boundary where routing meets the VLANs of access layer switches.
- Ex: 3550,3560,3750,4500 Switches
- Core Layer
- · Core Layer provides interconnectivity between all distribution layer switches.
- Core Layer is sometimes also called as Backbone must be capable of forwarding traffic from one distribution layer to other distribution layer switch as efficiently as possible
- Ex: 6500 Switch

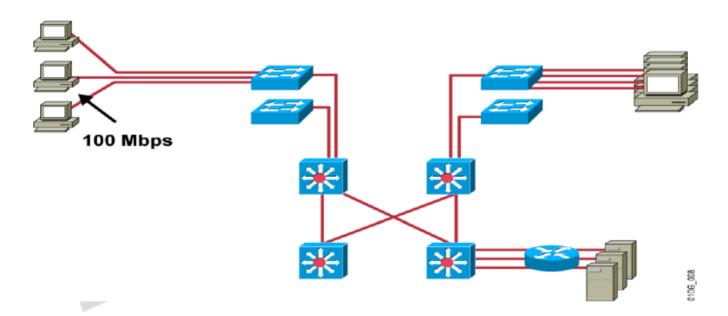






### **Fast Ethernet**





• Provides client access to the network

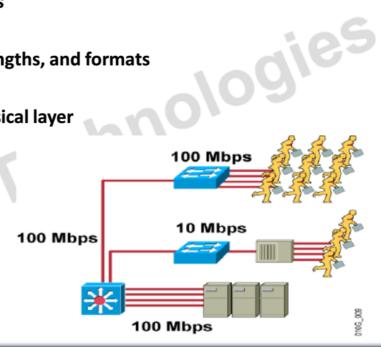




### **Fast Ethernet**



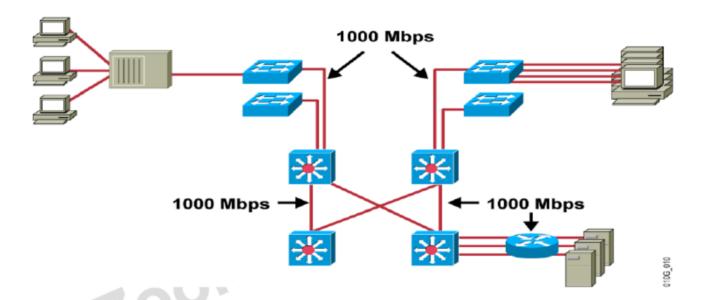
- Built on Ethernet principles
- Bandwidth 100 Mbps
- Uses same frame types, lengths, and formats
- Still CSMA/CD
- Same MAC layer, new physical layer





### **Gigabit Ethernet**



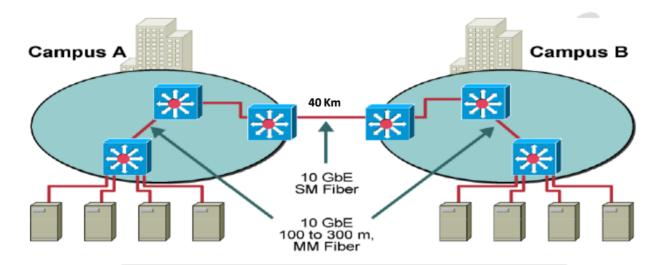


- Enhances client/server performance across the enterprise
- Connects distribution-layer switches in each building with a central campus core









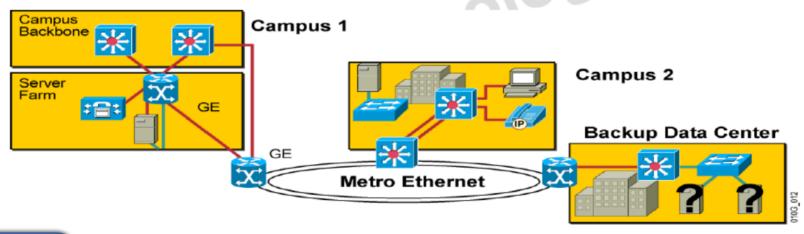
- Cost-effective bandwidth for the LAN, switch-to-switch
  Used to aggregate multiple Gigabit Ethernet segments
- 10 Gigabit EtherChannel will enable 20 to 80 Gbps (future)



### **Metro Ethernet**



- Leverages service provider network or existing, unused optical fiber (dark fiber) for metro Ethernet connectivity
- Supports any IP application







### **Switching Types**



- Zoom Technologies · Store and Forward
- Cut Through
- Fragment Free



### **Store and Forward**



FCS L3, L4, and Data	Ether Type	Source MAC	Dest. MAC
----------------------	---------------	------------	-----------



In Store and Forward switching, Switch copies each complete frame into the switch memory and performs CRC(cyclic Redundancy Check) on that frame. If there are any errors it will drop that frame, if there are no errors it will forward the frame.

Delay is high, number of frames forwarded is low when compared to other types of switching







FCS L3, L4, and Data	Ether Type	Source MAC	Dest. MAC
----------------------	---------------	------------	-----------



In cut-through switching, the switch copies only the destination MAC address (first 6 bytes of the frame) of the frame into its memory before making a switching decision.

More Errors - because it is not performing CRC.

Low Delay



### **Fragment Free**

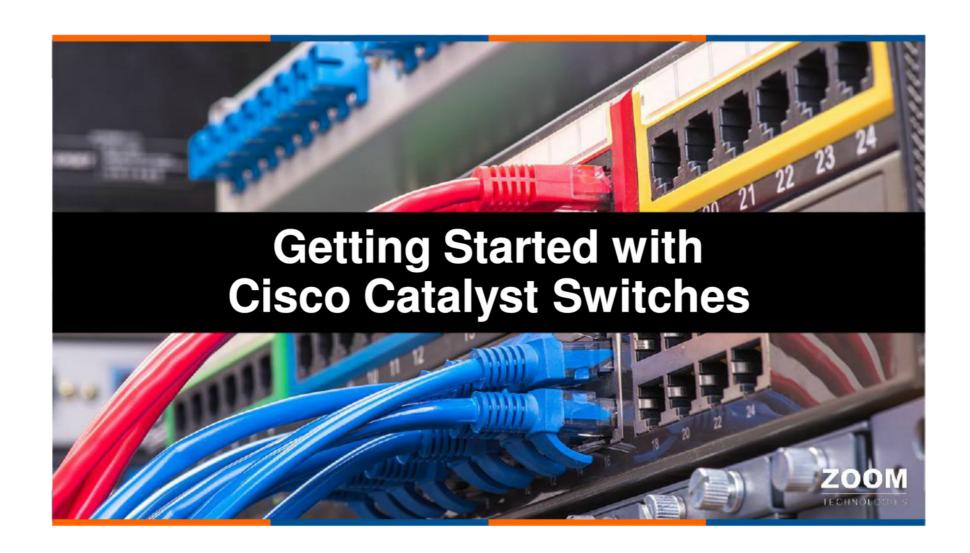




Fragment-free (runtless switching) switching is an advanced form of cut-through switching. The switches operating in fragment-free switching read at least 64 bytes of the Ethernet frame before switching it to avoid forwarding Ethernet runt frames(Ethernet frames smaller than 64 bytes).







### **Cat OS and Cisco IOS (Native Mode)**



- Cat OS
  - Layer 2 switching functions
- Hybrid Mode
  - Cat OS for Layer 2 switching
  - IOS for Layer 3
- Cisco IOS (Native Mode)
- mologies Works for both Layer 2/Layer 3 switching
  - Runs on a device that can have a port that acts like a router port (Layer 3) or like a switched port (Layer 2)
  - Available on all new Catalyst switches





### **CAM VS TCAM**



### **CAM Table**

CAM Table is used to store layer 2 information like

- Source MAC address
- nologies Interface where we learned the source MAC address
- Vlan information

### **TCAM Table**

TCAM table is used to store higher information like

- Access-list
- QOS
- Routing Table



### **CDP Cisco Discovery Protocol**



- CDP is a Layer 2 protocol used to find information about neighbor devices
- CDP Advertisements are sent as multicast frames.
- By default CDP is enabled on all Cisco devices.
- If an attacker is listening to CDP messages, it could learn important information about the device model and the current software version

ologies

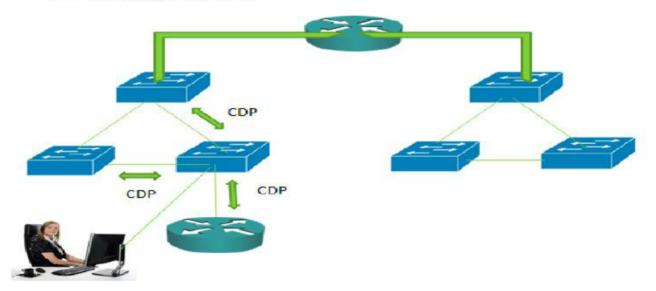
Note: Cisco recommends disabling CDP when not in use.







 To get the information about neighbors by using CDP #show cdp neighbors





### **LLDP**



- LLDP is similar to CDP but works on multi vendor networks.
- LLDP is an IEEE 802.1AB standard
- echnologies By default LLDP is disabled on Cisco devices.
- To enable LLDP on a Cisco device

Switch(conf)#Ildp run







### **Virtual LANs**



- VLANs are used to divide one large broadcast domain into multiple smaller broadcast domains.
- A large network can be divided into VLANs based on Project, Department or function etc.
- VLANs provide Broadcast Segmentation
- Each VLAN is a single Broadcast domain







### Static Dynamic Switch Switch Switch Switch Switch



### **Static VLANS**



- Static Vlans are also called as port-based vlans.
- · Any device connecting to the port will become a member of that Vlan.
- This is the most common method of assigning ports to VLANs
- There is a default VLAN, on Cisco switches :VLAN 1





### **Dynamic Vlan**



- Dynamic Vlans are also called MAC based vlans.
- Vlans are automatically created by switch and assigned as per the mac address of the connected device.
- Dynamic vlans are flexible compared to static vlans.
- VMPS is required to configure Dynamic Vlans.

200m



### **Voice Vlan**



- Voice Vlan allows access ports to carry voice traffic from an IP phone
- By default voice vlan feature is disabled.
- · To enable, Give the following command

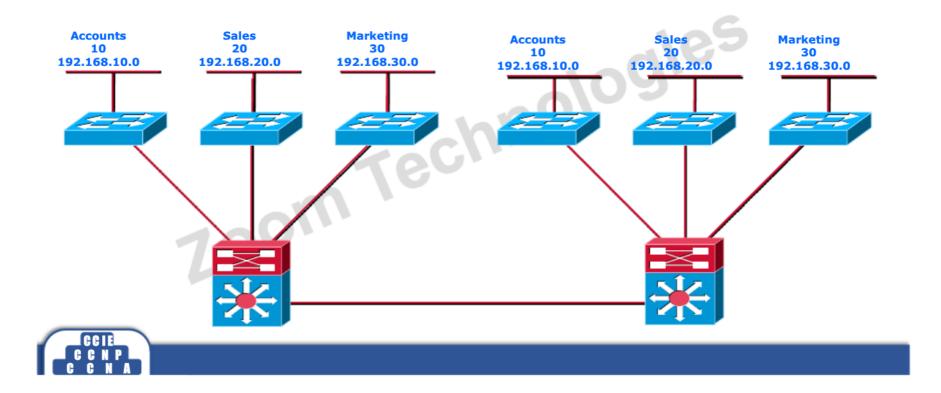
...10 TeChnologies Switch(conf-if)# switchport voice vlan 10





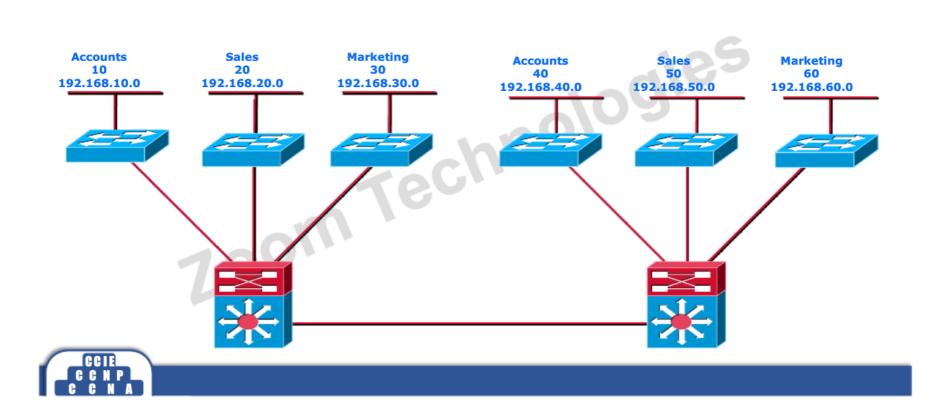
### **End to End Vlan**





### **Local Vlan**









	VLAN Range	Range	Usage
	1	Normal	Cisco default
	2-1001	Normal	For Ethernet VLANs
	1002-1005	Normal	Cisco defaults for FDDI and Token Ring
	1006-4094	Extended	For Ethernet VLANs
_GeTi_			
C C N P			

### **Creating a VLAN**



Switch(config)#Vlan <no>

Technc Switch(config-vlan)#name < name >







### Switch(config)#interface gigabitethernet 1/1

Enters interface configuration mode

### Switch(config-if)#switchport mode access

Configures the interface as an access port

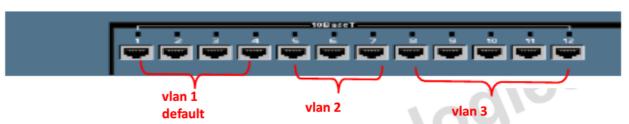
### Switch(config-if)#switchport access vlan 3

Assigns the access port to a VLAN



### Verifying VLANs – show vlan





Sydne	ySwitch# <b>show vlan</b>						
VLAN	Name	Status	Ports				
VLAN	Name	Status	Ports				
1	default	active	Fa0/1,	Fa0/2,	Fa0/3,	Fa0/4	
2	VLAN2	active	Fa0/5,	Fa0/6,	Fa0/7		
3	VLAN3	active	Fa0/8, Fa0/12	Fa0/9,	Fa0/10,	Fa0/1	1,
1002	fddi-default	active					
1003	token-ring-default	active					
1004	fddinet-default	active					
1005	trnet-default	active					
MAIV	Type SAID MTU Pare	nt RingNo	BridgeNo	Stp Bı	dgMode	Trans1	Trans2
T .	enet 100001 1500 -	_	_	_	_	1002	
2	enet 100002 1500 -	_	_	_	_	0	0





```
S1# conf t
S1(config) # no vlan 20
S1(config) # end
S1#
S1# sh vlan brief

VLAN Name

I default

Status

Status

Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gi0/1

1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default
1005 trnet-default
1006 sat/unsup
1007 act/unsup
1008 act/unsup
1009 act/unsup
```

### Switch(config-if)#no switchport access vlan vlan\_number

- This command will reset the interface to VLAN 1.
- VLAN 1 cannot be removed from the switch.





### **Trunking Encapsulation**

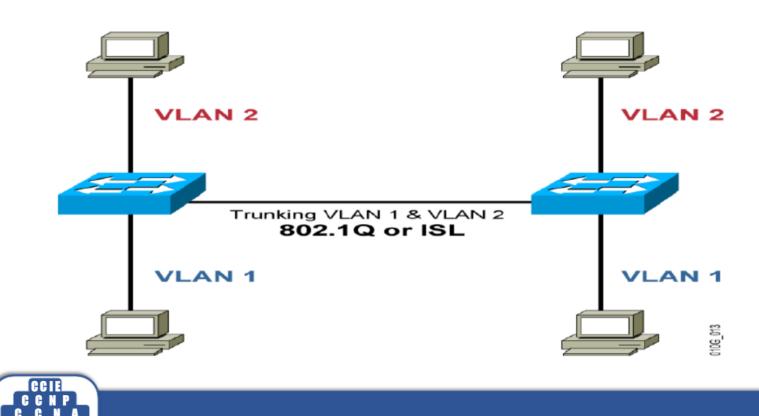


- · VLANs are local to each switch's database, and VLAN information is not passed between switches. Trunks carry traffic from all VLANs to and from the switch by default ...(C) but can be configured to carry only specified VLAN traffic.
- Two types of trunking encapsulation protocols
- ISL(Inter Switch Link)
- 802.1Q( Dot 1Q)



### **VLAN Trunk Encapsulation**



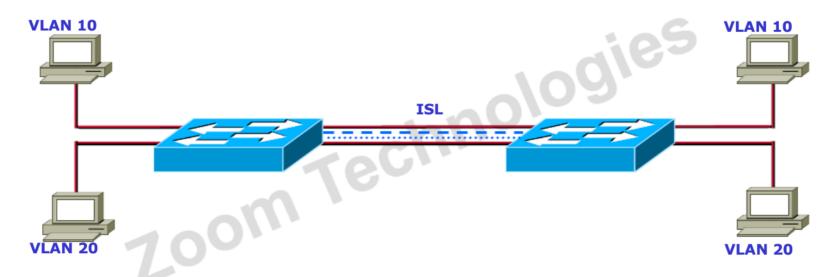




### **ISL Encapsulation**









### **ISL and Layer 2 Encapsulation**



### ISL Encapsulated Layer 2 Frame from an ISL Trunk Port

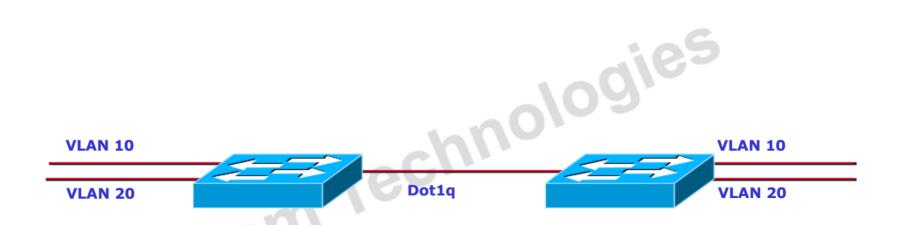
ISL Header (26B)	DA (6B)	SA (6B)	Length/ Etype (2B)	Data (0-1500 Bytes)	FCS (4B)	ISL FCS (4B)
Untagged a	ind Une	ncapsı	ılated Layer	· 2 Frame from an Access I	Port	-

(6B) (6B) (2B) (0-1500B) (4B)		DA (6B)	SA (6B)	Len/Etype (2B)	Data (0-1500B)	FCS (4B)
-------------------------------	--	------------	------------	-------------------	-------------------	-------------











802.1Q



### 802.1Q Tagged Layer 2 Frame from an 802.1Q Trunk Port

DA (6B)	Etype (8100) (2B)		Dot1Q Trunk Tag (2B)	Length/ Etype (2B)	Data (0-1500 Bytes)	FCS (4B)
------------	-------------------------	--	-------------------------	--------------------------	------------------------	-------------

### Untagged and Unencapsulated Layer 2 Frame from an Access Port

DA	SA	Len/Etype	Data	FCS	9105_018
(6B)	(6B)	(2B)	(0-1500B)	(4B)	





# Importance of Native VLANS 10.3.3.1 the property of 10.3.3.2 VLAN2 802.1Q 802.1Q VLAN2 10.2.2.2 10.1.1.1 10.1.1.2

### **Configuring Trunk link**



### Switch(config)#interface fastethernet 2/1

• Enters interface configuration mode

### Switch(config-if)#switchport trunk encapsulation isI/dot1q

• Selects the encapsulation

### Switch(config-if)#switchport mode trunk

Configures the interface as a Layer 2 trunk





### **Verifying Trunking**



Switch#show running-config interface {fastethernet | gigabitethernet} slot/port

Switch#show interfaces [fastethernet | gigabitethernet] slot/port [ switchport | trunk ]

### Switch#show interfaces fastethernet 2/1 trunk

**Native VLAN** Port Mode **Encapsulation Status** 

Fa2/1 desirable isl trunking

Port VLANs allowed on trunk

Fa2/1 1-1005

VLANs allowed and active in management domain Port

1-2,1002-1005 Fa2/1

Port VLANs in spanning tree forwarding state and not pruned

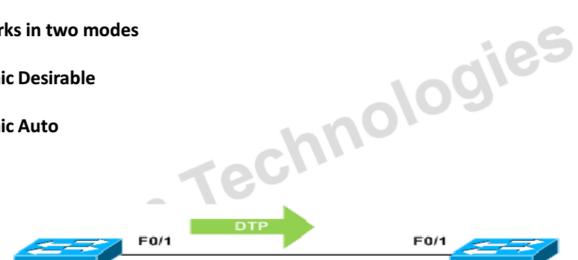
Fa2/1 1-2,1002-1005



### **Dynamic Trunking Protocol**



- Dynamic Trunking protocol is a dynamic way of establishing a trunk between two switches.
- **DTP works in two modes**
- 1) Dynamic Desirable
- 2) Dynamic Auto



F0/1

interface FastEthernet0/1 switchport mode dynamic desirable

interface FastEthernet0/1 switchport mode dynamic auto





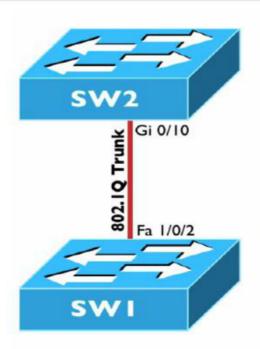


Switch(conf)#interface fastethernet 0/1
Switch(conf-if)#switchport nonegotiate



### **Switchport Modes**



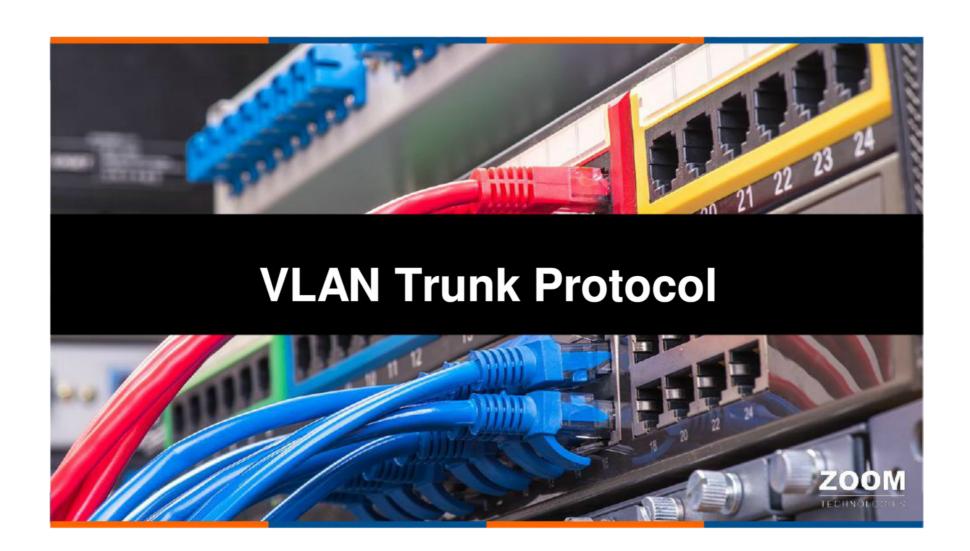


Mode	Description		
access	Forces a port to operate as an access port.		
trunk Forces a port to operate as a trunk port.			
dynamic desirable	Initiates the negotiation of a trunk.		
dynamic auto	Passively waits for the remote switch to initiate the negotiation of a trunk		

SWI Mode	SW2 Mode	Trunk Formed
access	ANY	×
trunk	dynamic desirable	*
trunk	dynamic auto	<b>√</b>
trunk	trunk	*
dynamic desirable	dynamic desirable	*
dynamic desirable	dynamic auto	*
dynamic auto	dynamic auto	







### **Purpose of VTP**

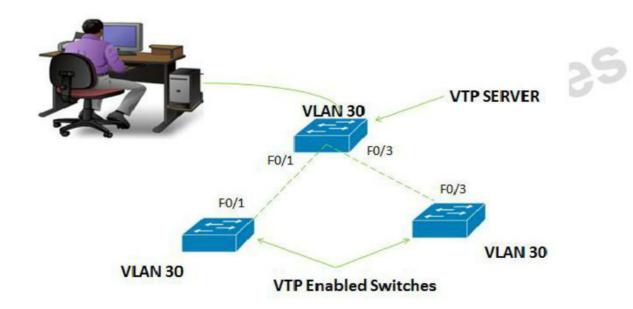


- You can create VLANs on a switch.
- What if you have the same VLANs on 10 linked switches? Or 100 linked switches?
- Do you have to create the VLANs on every switch and allow them on each trunk?
- VTP helps.
- But you still have to assign access ports to VLANs on each switch.











### **VTP Protocol Features**



- VTP is a Cisco proprietary protocol.
- VTP is used to exchange vlan information between switches.
- Sends VTP advertisements on trunk ports only
- VTP reduces administration in a switched network.
- Maintains VLAN configuration consistency throughout a common administrative domain

Note: VTP will not assign vlan's to the ports.





### **VTP Modes**



### **VTP Server**

- Create Vlans
- Delete Vlans
- Modify Vlans
- Sends and Forwards Advertisements
- Synchronizes

### **VTP Client**

- echnologies (lar Cannot create, delete and modify Vlans
- Forward Advertisements
- Synchronizes



### **VTP Modes**



### **VTP Transparent**

- Zoom Technologies Create, delete and modify Vlans local to the switch
- Forward Advertisements
- Does not synchronize





#### **Configuration Revision Number**

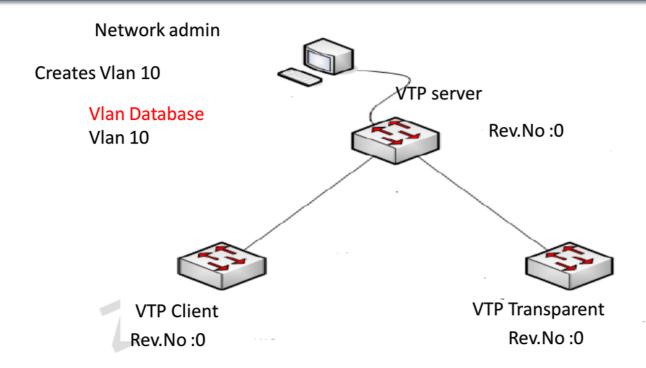


- VTP works based upon configuration revision number.
- Configuration revision number increases by one every time we create, delete and modify vlans on the sever.
- Configuration revision number ranges from 0-65,535
- This ensures that each switch participating in VTP always has the latest information comparing the current configuration revison number with the received update, the update will be accepted only if it has a greater configuration revision number
- Configuration revision number of transparent switch always zero.



#### **Working of VTP**



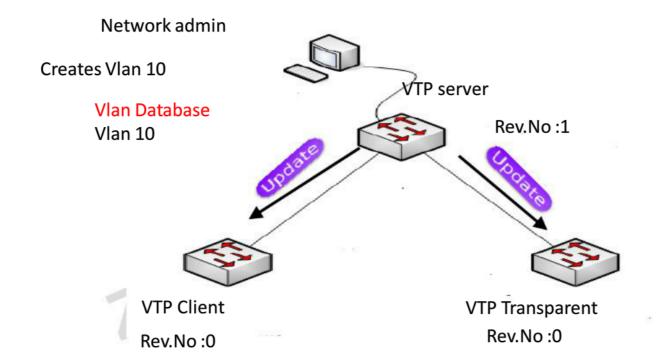






# **Working of VTP**

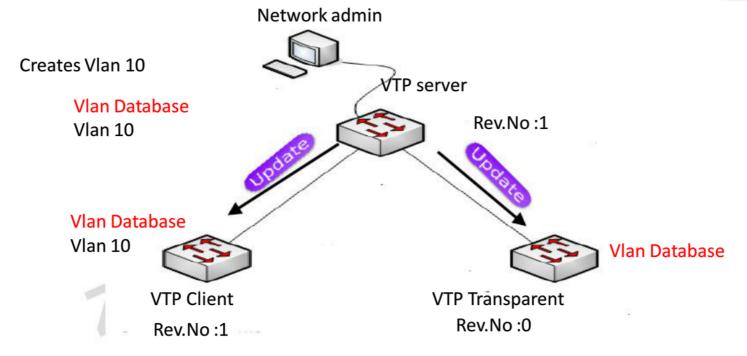






# **Working of VTP**





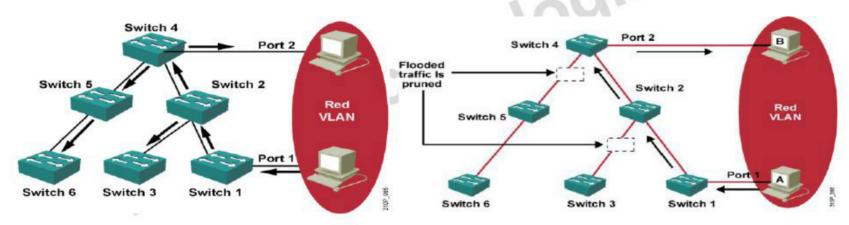




#### **VTP Pruning**



- · Uses bandwidth more efficiently by reducing unnecessary flooded traffic
- Example: Station A sends broadcast; broadcast flooded only toward any switch with ports assigned to the red VLAN



**Pruning Disabled** 

**Pruning Enabled** 



#### **Configuring a VTP Server**



Switch(config) #vtp mode server

Configures VTP server mode

Switch(config) #vtp domain domain-name

Specifies a domain name

Switch(config) #vtp password password

Sets a VTP password

Switch (config) #vtp pruning

Enables VTP pruning in the domain





#### **Verifying the VTP Configuration**



#### Switch#show vtp status

#### Switch#show vtp status

VTP Version : 2 Configuration Revision : 247 Maximum VLANs supported locally: 1005 Number of existing VLANs : 33 : Client VTP Operating Mode

VTP Domain Name : Lab Network VTP Pruning Mode : Enabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled

: 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80 MD5 digest

Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49



#### **VTP Advertisements**



#### 1) Summary Advertisements





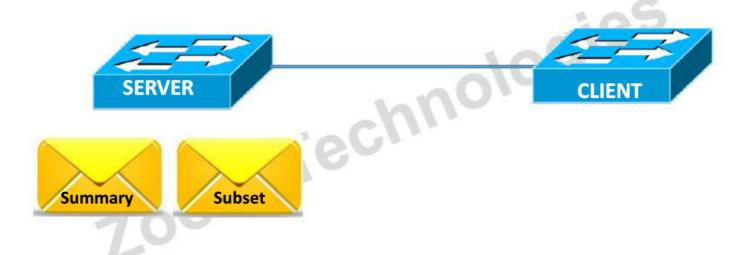




#### **VTP Advertisements**



#### 2) Subset Advertisements

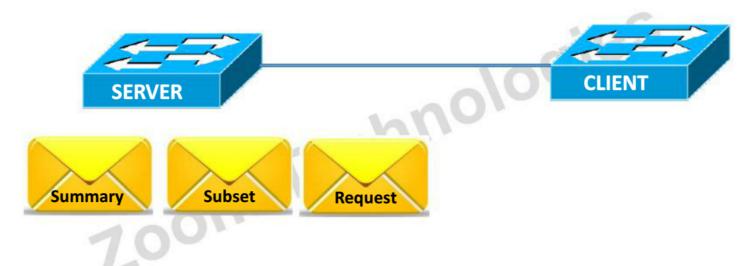




#### **VTP Advertisements**



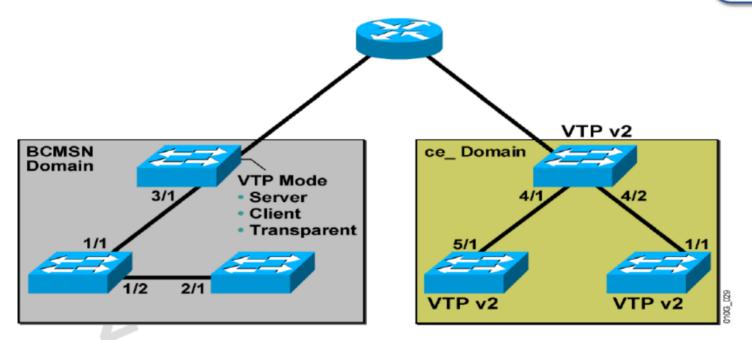
# 3) Request Advertisement











All switches in a management domain must run the same version.



#### Problem in VTP Version 1 and 2



- In VTP version 1 and2, VTP client can override vlan information in VTP server if it has higher configuration revision number compared to server.
- It is recommended to add new switch to the switched network in VTP client with revision number zero.
- VTP version 3 overcomes this problem
- VTP version 3 supports password encryption.



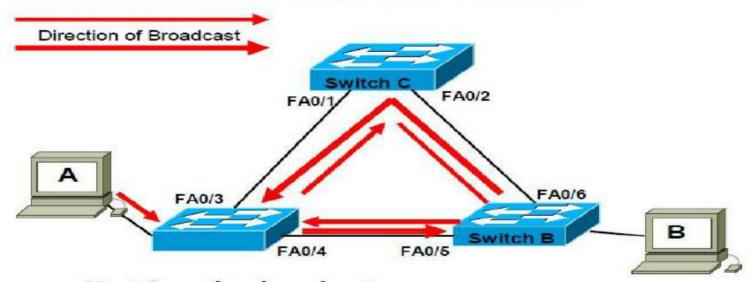




# **Bridging Loops**



# **Broadcast Storm**



- Host A sends a broadcast.
- Switches continue to propagate broadcast traffic over and over

#### **Spanning Tree Protocol**



- STP is open standard protocol(IEEE 802.1D)
- It blocks all the redundant paths and provides a loop free L2 path
- STP uses Spanning Tree Algorithm(STA) to provide loop free topology
- alg Zoom Technoli "Radia Perlman" is the inventor of the spanning tree algorithm
- **Enabled by default on all Cisco switches**





#### **STP Election**



- Election of Root Bridge
- Lowest Bridge ID ( MAC address + Priority)
- Election of Root Port on Non Root Switch
- .ritch) Lowest Path cost (total cost to reach root switch)
- · Lowest sender bridge id
- Lowest Port ID (Port Number)
- Election of Designated Port on Non Root Switch
- Lowest Path cost
- Lowest sender bridge id
- Lowest Port ID



# **STP Cost**

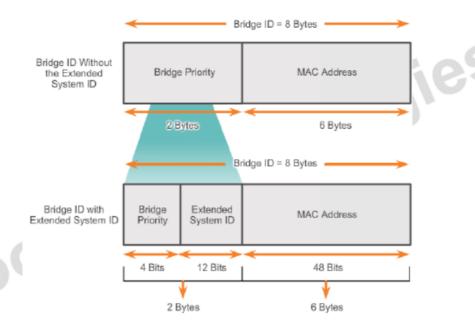


Speed	Cost		
10 Mbps	100		
100 Mbps	19		
1000 Mbps	4		
10000 Mbps	2		
7.00m			



# **Bridge ID**

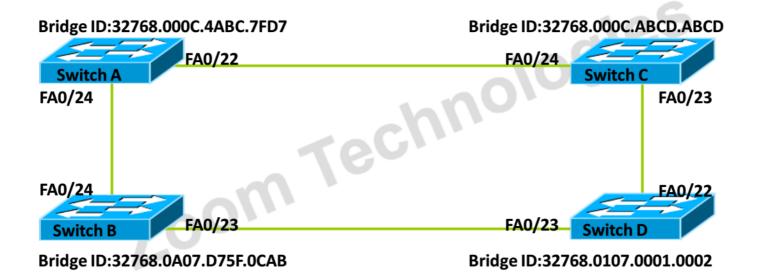




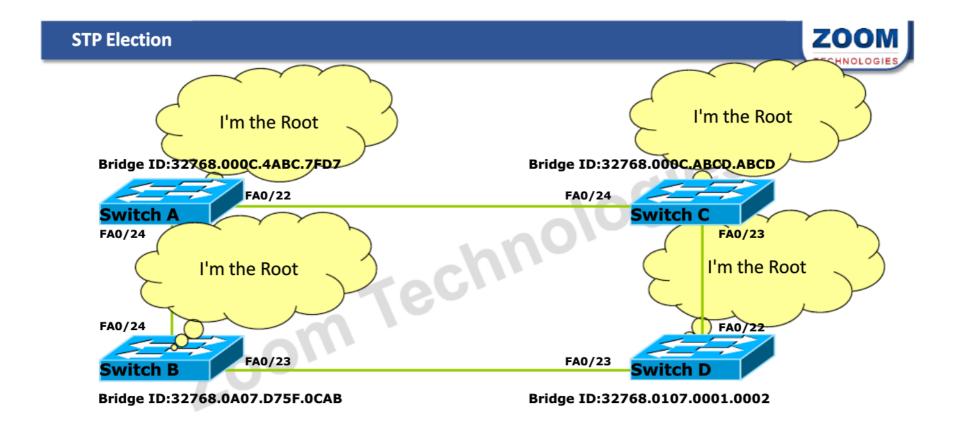










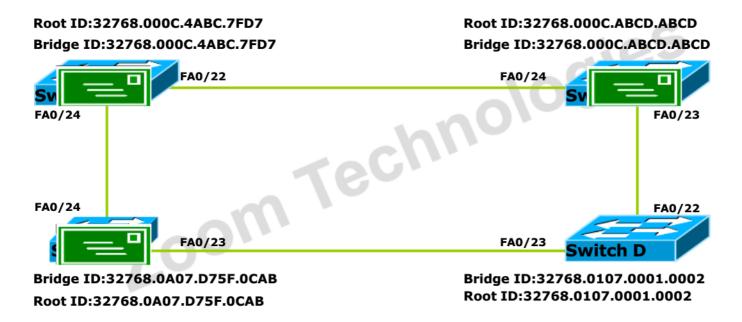






#### **STP Election**

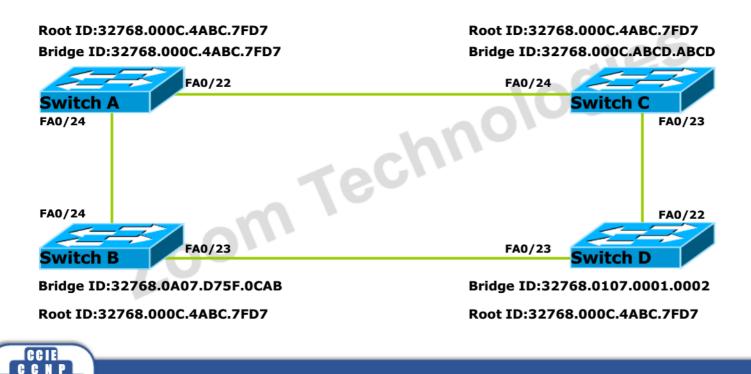






#### **STP Election**

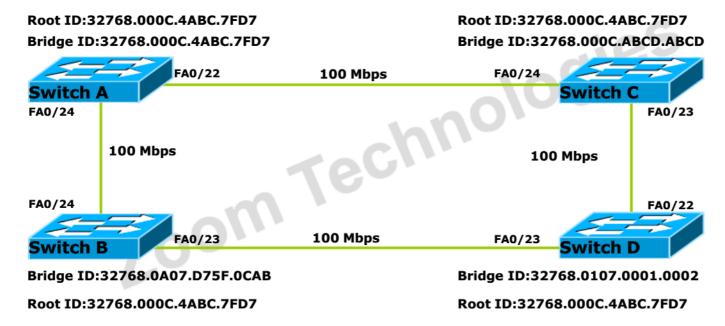






#### **STP Election**

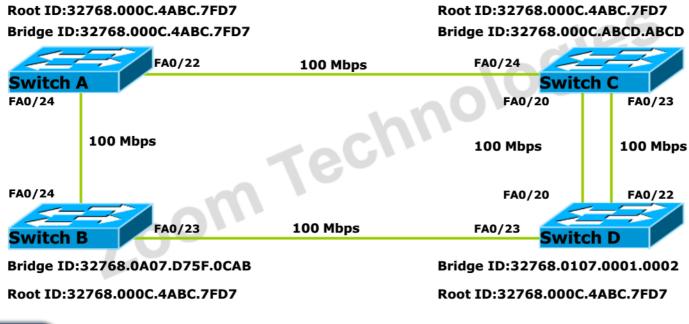






#### **STP Election**



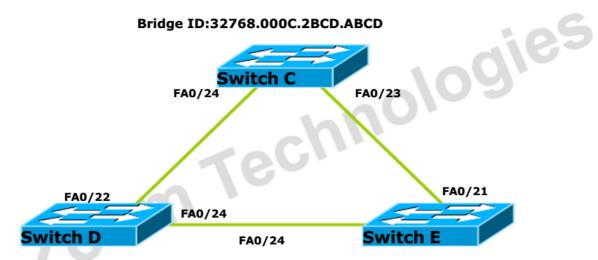








Bridge ID:32768.000C.2BCD.ABCD



Bridge ID:32768.000C.4ABC.ABCD

Bridge ID:32768.0000.000C.ABCD



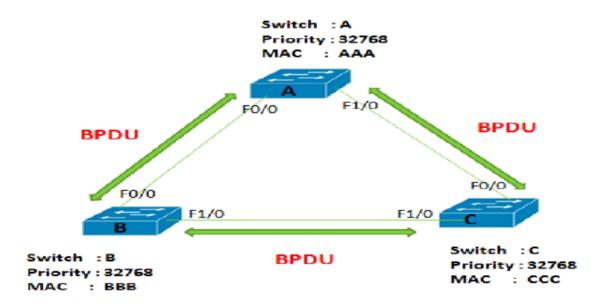
#### **BPDU**



- STP uses BPDU's(Bridge Protocol Data Unit) to find Switches send BPDU frame on multicast address 01:80:C2:00:00:00



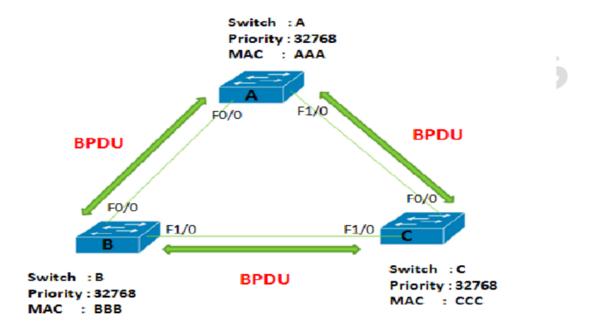






# **BPDU** exchange







# **Types Of BPDUs**



- Configuration BPDU
- Topology Change Acknowledgement BPDU



#### **BPDU**



Protocol	Version	Message type	Root ID	Cost	Bridge ID	Port ID	Message Age	Max Time	Hello	Forward Delay
1 B	1 B	1 B	8 B	4 B	8 B	2 B	2 B	2 B	2 B	2 B
Zoom Techno.										





#### **STP Port States**



- Disabled State:
  - · Layer 2 port does not participate in spanning tree and does not forward echnologies 's frames.
- Blocked State:
  - Only receives BPDU's
  - · Stays for 20 sec
- · Listening State:
  - Receives and Sends BPDU's
  - Stays for 15 sec



#### **STP Port States**



- Learning State:
  - Receives and Sends BPDU
  - Learns Mac address
  - Stays for 15 sec
- Forwarding State:
- rechnologies Receives and Sends BPDU
  - Learns Mac address
  - Forwards data room



#### **STP Timers**



#### Hello Timer

Determines how often root bridge sends configuration BPDUs. The default is 2 seconds.

#### Max Age

how long to keep ports in the blocking state before listening. The default is 20 seconds.

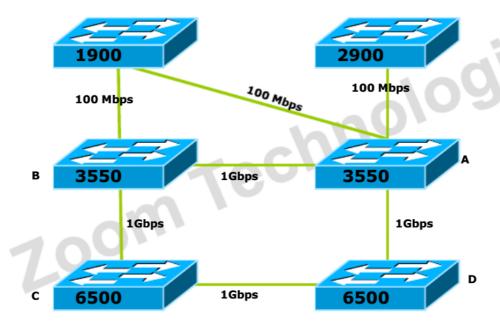
#### Forward Delay

 how long to stay in the listening state before going to the learning state, and how long to stay in the learning state before forwarding. The default is 15 seconds.



#### **Planning Root Bridge**











#### **Enhancements to STP**

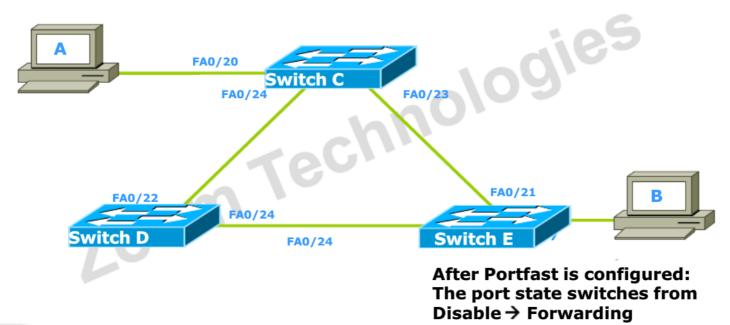


- Portfast
  - used for Access ports
  - port state switched from Disable to Forwarding
  - No delay, saves 50 seconds
- Uplinkfast
  - configured on a switch with at least one Blocked port
  - the Blocked port switches to Forwarding state without any delay, saves 30 seconds
- Backbonefast
  - · configured on all switches
  - if indirectly connected link fails, the switch with Blocked port switches to Forwarding state in 30 seconds, saves 20 seconds





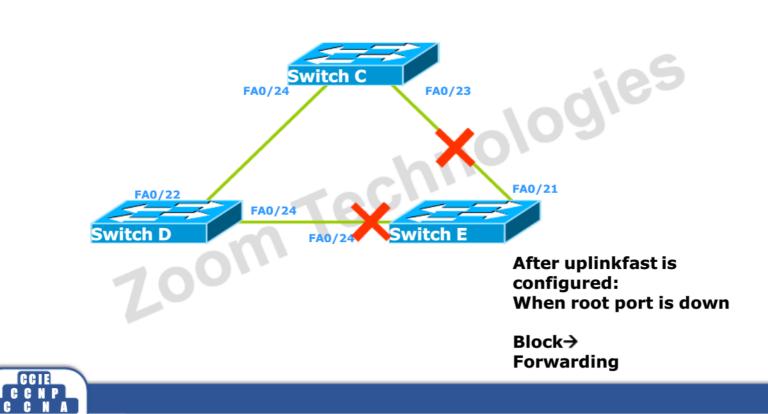






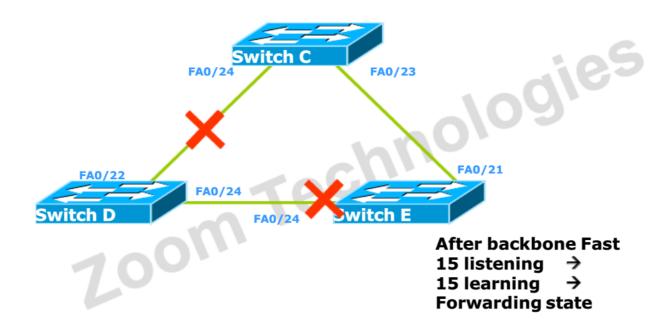
#### **STP Uplinkfast**















#### **PVST**

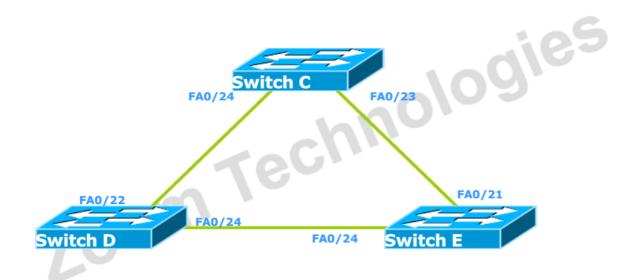


- Cisco proprietary
- Single STP instance for each VLAN
- PVST work only on trunk link
- 7.000 Technologies PVST works only ISL, PVST+ works on ISL/Dot1Q



**PVST** 

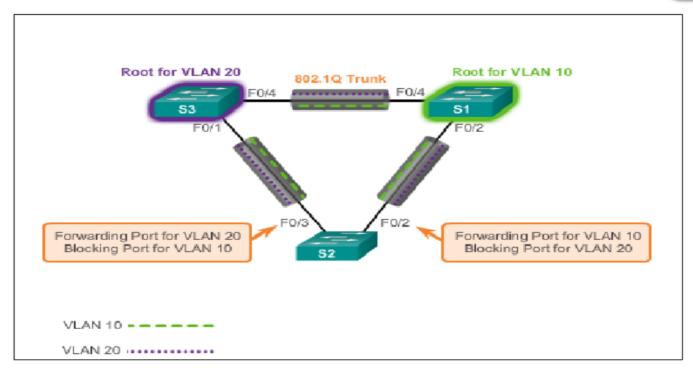
















# **Rapid Spanning Protocol**



- Open Standard (IEEE 802.1w)
- · RSTP is enhanced version of STP
- RSTP Election Process is similar to STP

700m

- RSTP is backward compatible with STP 802.1D
- RSTP provides faster convergence
  - BPDU is send every 2 sec and hold 6 sec
- ologies Uplinkfast and Backbonefast are enabled by default



#### **RSTP Port States**



STP	RSTP		
Disable	1.6		
Blocked	Discarding		
Listening	700,		
Learning	Learning		
Forwarding	Forwarding		
7.00m Tev			





#### **RSTP Port States**



#### **Port States**

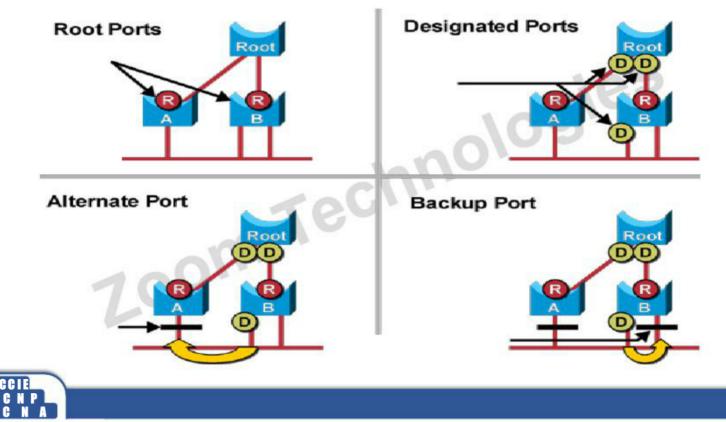
- Discarding
- Learning
- Learning
  Accepts data frames to populate the MAC table.

  Forwarding
  Forwards data frames Forwarding



#### **RSTP Port Roles**







# **RSTP Port Type**



- · Link Type in RSTP are
  - Edge port:
    - mologies · Port configured with Portfast command
  - Non Edge Port:
    - · Port without a Portfast command
    - Non Edge port are of two type:
      - Point to Point : Full Duplex links
      - Shared: Half Duplex Link

700m





#### **MST**



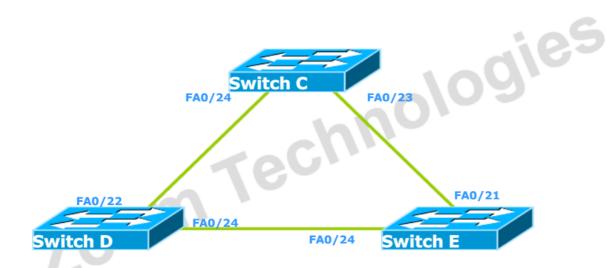
- Open Standard (IEEE 802.1s)
- One STP for a group of VLAN
- , ree 01091e5 Also Know as Multiple instance of Spanning tree
- Backwards compatible with STP and RSTP

700m



**MST** 

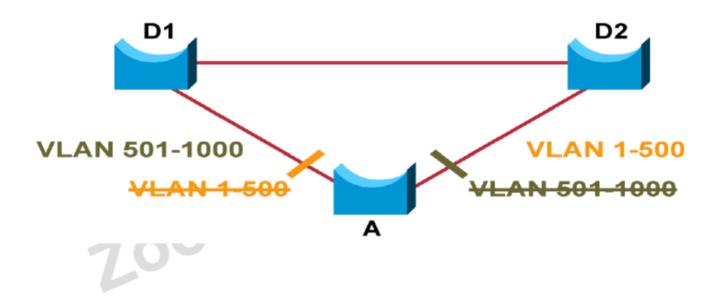










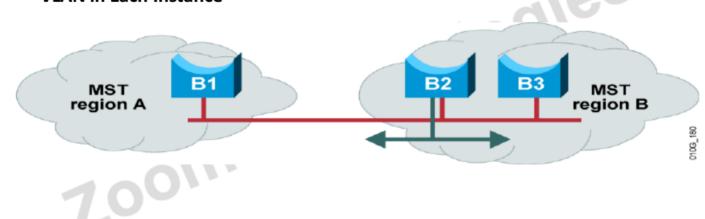




# **MST Regions**



- MST configuration on each switch:
  - Name
  - Revision number
  - VLAN in Each Instance

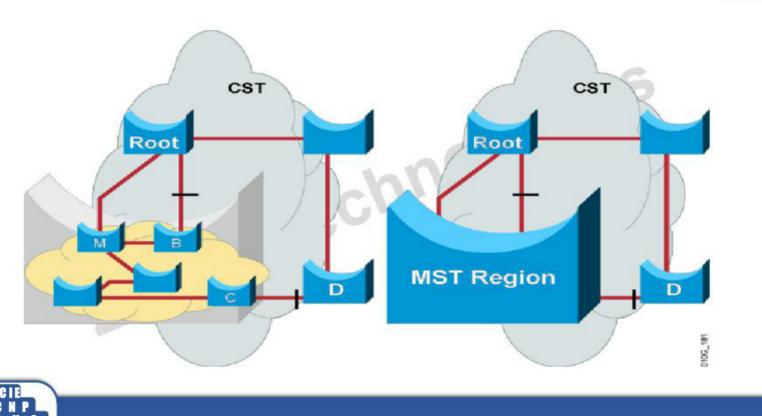






# **MST Backward Compatibility**





# **Enabling Multiple Spanning Tree**



# Zoom Technologi Zoom Switch(config)#spanning-tree mode mst

• Enables Multiple Spanning Tree







#### Switch(config)#spanning-tree mst configuration

Enters MST configuration submode

#### Switch(config-mst)#name name

Sets the MST region name

#### Switch(config-mst)#revision rev\_num

Sets the MST configuration revision number

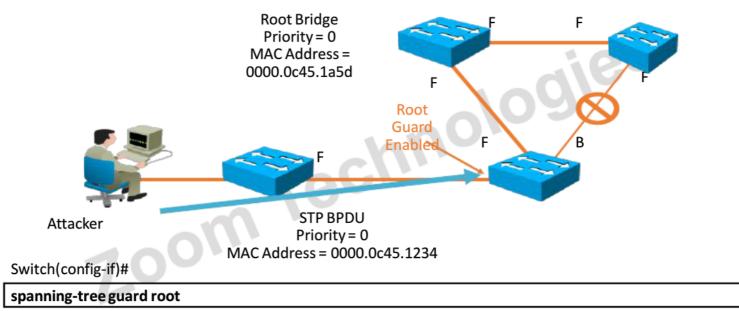
#### Switch(config-mst)#instance inst vlan range

Maps the VLANs to an MST instance









· Enables root guard on a per-interface basis



#### **BPDU** guard

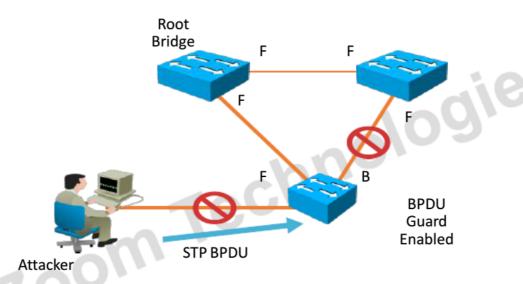


- BPDU guard places a PortFast port into blocking state if a BPDU is received on that port
  - · If a switch is attached to a port configured with Port Fast a layer 2 loop may occur, followed by a broadcast storm Protects a port configured with PortFast









Switch(config)#

spanning-tree portfast bpduguard default

· Globally enables BPDU guard on all ports with PortFast enabled



#### **BPDU Filter**



- BPDU Filtering allows a switch to stop sending/receiving BPDUs on a port depending on how is configured.
- BPDU Filtering configured on the interface level will completely stop sending and receiving of BPDU.
- BPDU Filtering configured on the Global configuration level will remove the port fast state and transition the port through normal STP states.
- SwitchB(config-if)#spanning-tree bpdufilter enable







#### **Loop Guard**



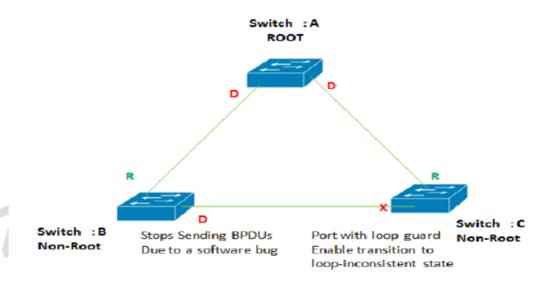
- Loop guard helps prevent bridging loops that could occur because of Software and Hardware failure
- High CPU utilization may prevent BPDUs from being received or processed.
- Loop Guard will place the interface in the loop-inconsistent state.
- Switch(config-if)# spanning-tree guard loop







# Loop Guard

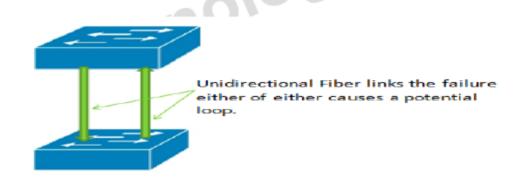




#### **UDLD**

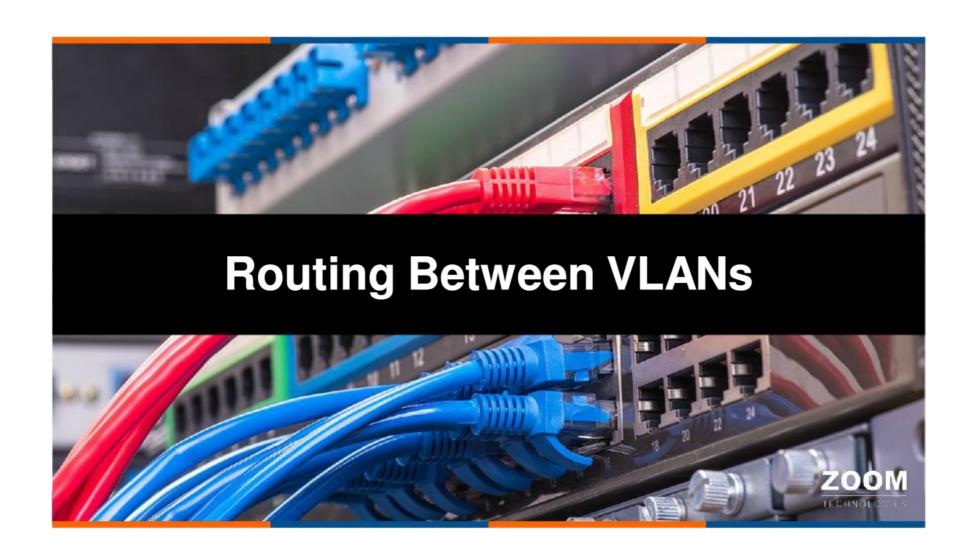


- UDLD is similar to loop guard used to prevent loops caused by unidirectional links.
- UDLD is typically used on fiber links.
- Switch(config)#udld enable









#### **Inter Vlan Routing**



- By default Layer 2 switch cannot forward the traffic between two different vlans.
- diff • A layer 3 device is required to forward the traffic between two different vlans.
- · A layer 3 device can be
- Router
- Multi Layer Switch





#### **Inter Vlan Routing Methods**



- **Legacy Inter Vlan Routing** Zoom Technologies
- **Router On a Stick**
- Multilayer Switch



#### **Legacy Inter Vlan Routing**



- It is also called as traditional inter vlan routing.
- Uses Router to perform Inter Vlan Routing.
- · Each vlan is connected to different physical interface of the router.
- · Packets would arrive on the router through one interface, leave through another interface.
- Large networks with large number of VLANs require many router interfaces.





# 172.17.10.1/24 172.17.30.1/24 G0/0 G0/1 F0/5 VLAN 30

PC3

172.17.30.23



#### **Router On a Stick**



- The router-on-a-stick approach uses a different path to route between VLANs.
- · The Physical interface of the router is divided into one or more sub interfaces.
- Vlans are assigned to sub interfaces instead of physical interfaces.
- · Each sub interface is configured with an IP address for the VLAN it represents.
- Only one of the router's physical interface is used.

PC<sub>1</sub>

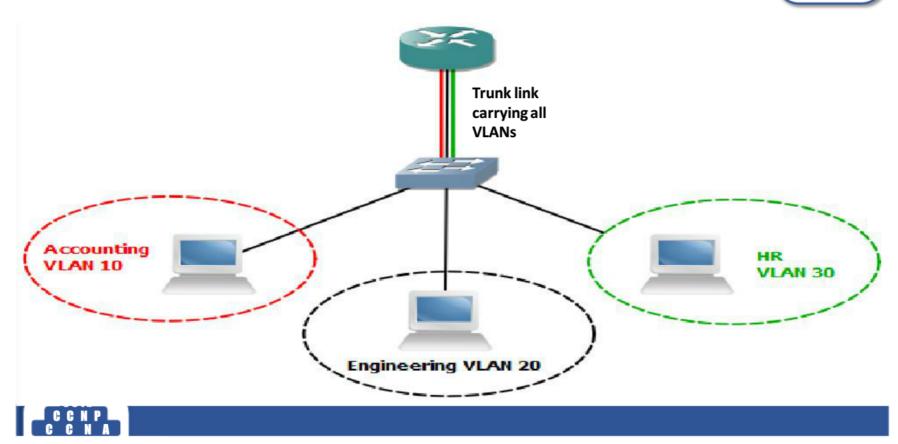
172.17.10.21





# **Router On a Stick**





# **Multi Layer Switching**



- Multi Layer Switch can perform layer 2 as well as layer 3 functions.
- Vlans are assigned to Switch Virtual Interface(SVI).

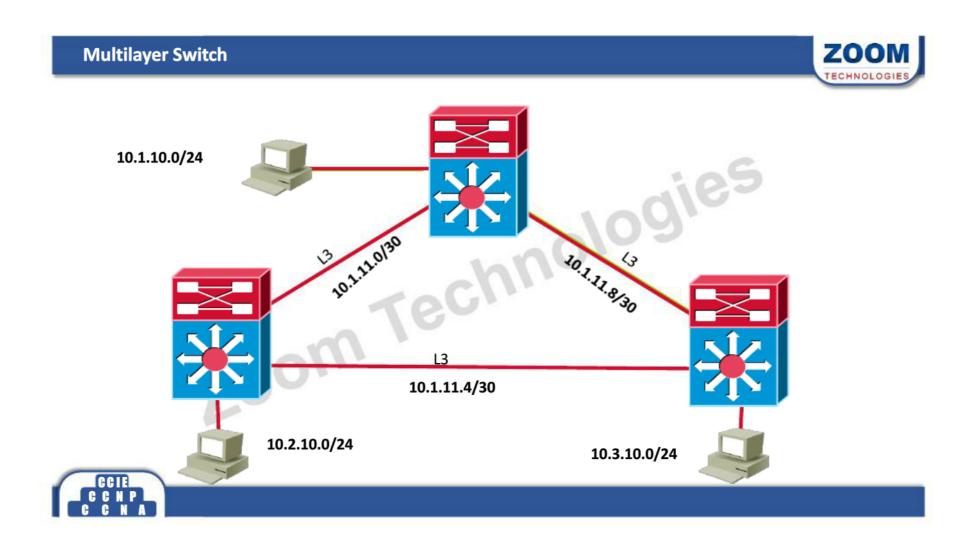
Zoom

- Each SVI is configured with an IP address for the VLAN it represents.
- This method uses ASIC to forward the traffic between vlans.





# Multi Layer Switching DIS-1 10.0.10.1/24 VIAN-10-10.0.30.1/34 VIAN-20-110.0.30.1/34 VIAN-30-110.0.30.1/34 VIAN-30-110.0.30.1/34 VIAN-30-110.0.30.1/34 VIAN-30-110.0.30.3/34 VIAN-30-10.0.30.3/34 VIAN-30-10.0.30.3/34 VIAN-30-10.0.30.3/34 VIAN-30-10.0.30.3/34 VIAN-30-10.0.30.3/34



# **Switch Port**



- The Switch port can work like Ethernet port on Router.
- ...k 1091eS By default the port works like Layer-2 port, we can enable it to work like Layer-3 port.
- To configure it
  - SW(config-if)#no switchport
  - **Assign IP and Subnet Mask**

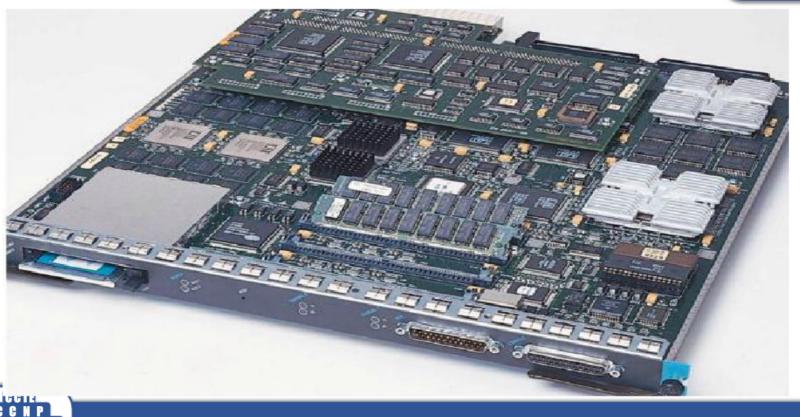
7.00m T

Router Port can be used in Routing protocols.

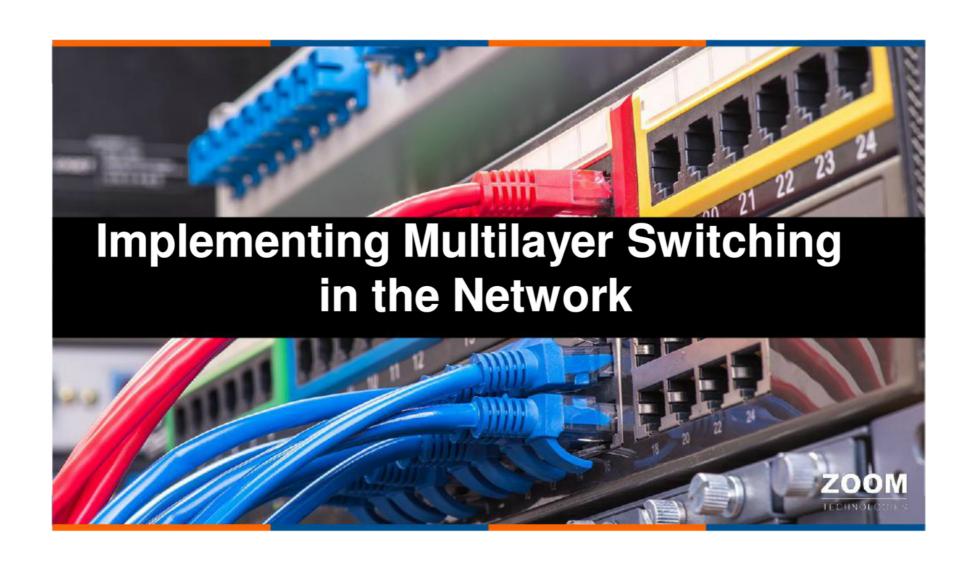


# **Supervisor Engine**



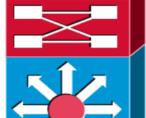






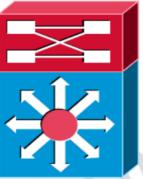
**Layer 3 Switching components** 





**Packet Switching: CEF ASIC** 

Layer 2 = layer 3 = layer 4



**Router Processing: Path Determination Load Balancing Multi Routing Protocol Support** 





# **Packet Switching Methods**



- **Process Switching**
- **Fast Switching**
- Zoom Technologies **CEF – Cisco Express Forwarding**



## **Process Switching**



- Process Switching is the oldest method of performing packet switching
- Process switching requires the CPU to be personally involved with every forwarding decision.
- The switching decision is made on a per packet basis
- Process switching is the slowest method of packet switching

To enable Process Switching

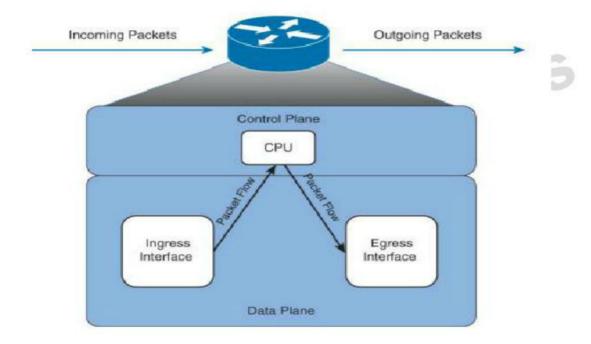
Router(conf-if)#no ip route-cache





# **Process Switching**







# **Fast Switching**



- Fast switching improves on process switching by making use of a cache
- The first packet to a destination is still process switched, Future packets to this destination
  will be switched using information from the fast cache, thus improving on the speed of
  this switching method.

To enable Fast Switching

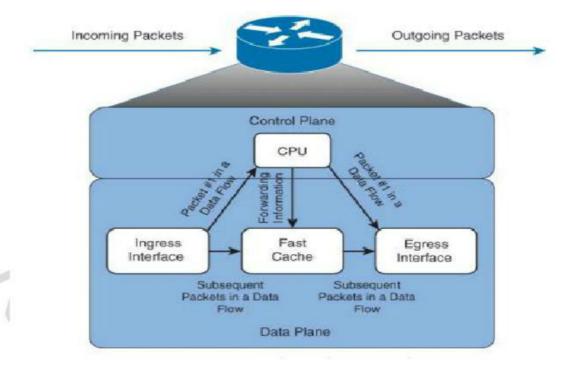
Router(conf-if)#ip route-cache





# **Fast Switching**







# **CEF – Cisco Express Forwarding**



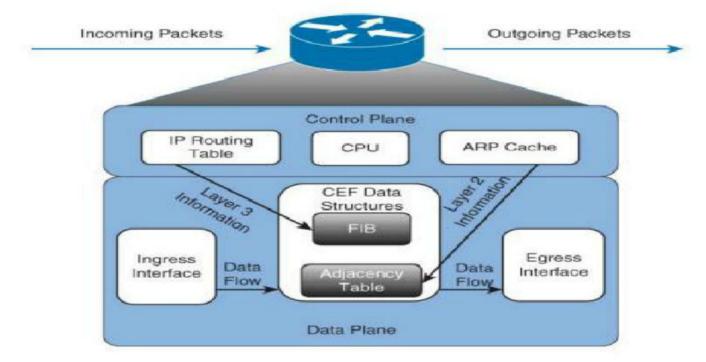
- CEF uses two components to perform packet switching
- Forward Information Base
- Adjacency Table
- Forward Information Base is similar to Routing Table, Adjacency Table is similar to ARP
   Table
  - To enable CEF

Router(conf-if)#ip route-cache cef











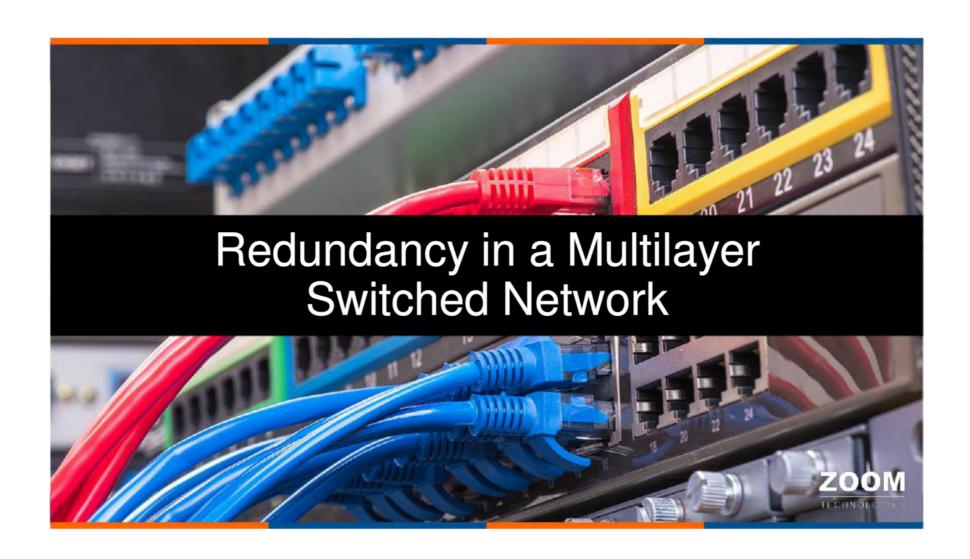
# **Displaying CEF Entries in the FIB**



dies

Switch#show ip cef [type/slot/port number] [detail]

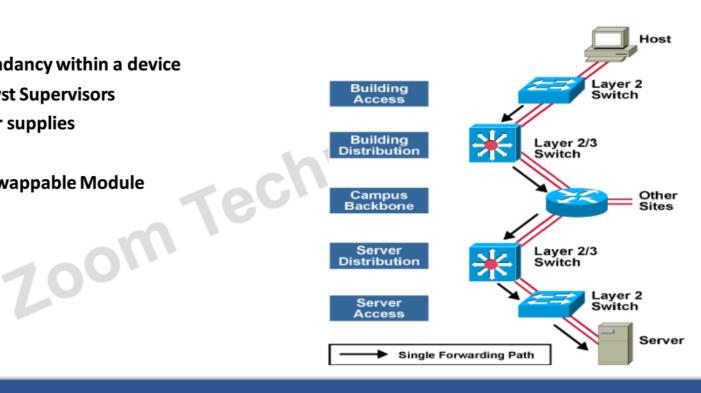




# **Single Points of Failure**



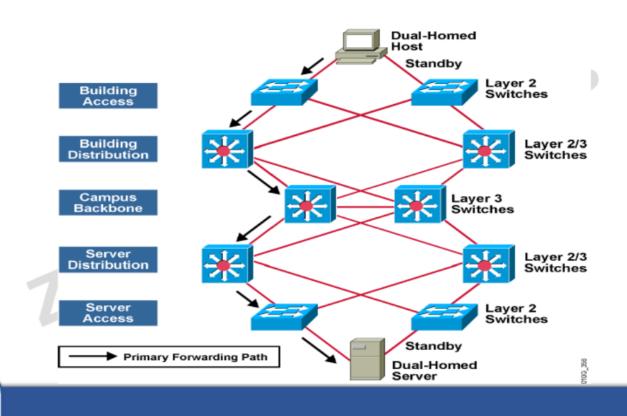
- Redundancy within a device
- **Catalyst Supervisors**
- **Power supplies**
- **Fans**
- **Hot-swappable Module**





# **Redundant Switched Network with No Single Point of Failure**

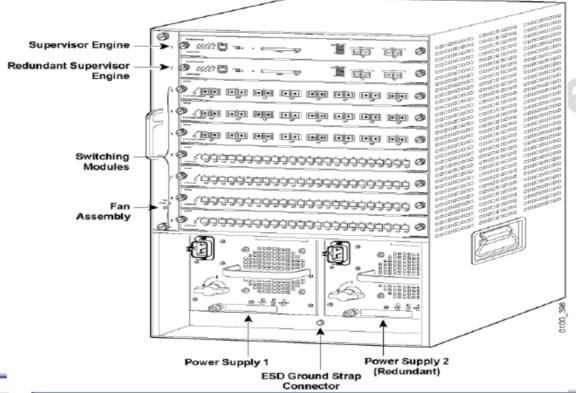




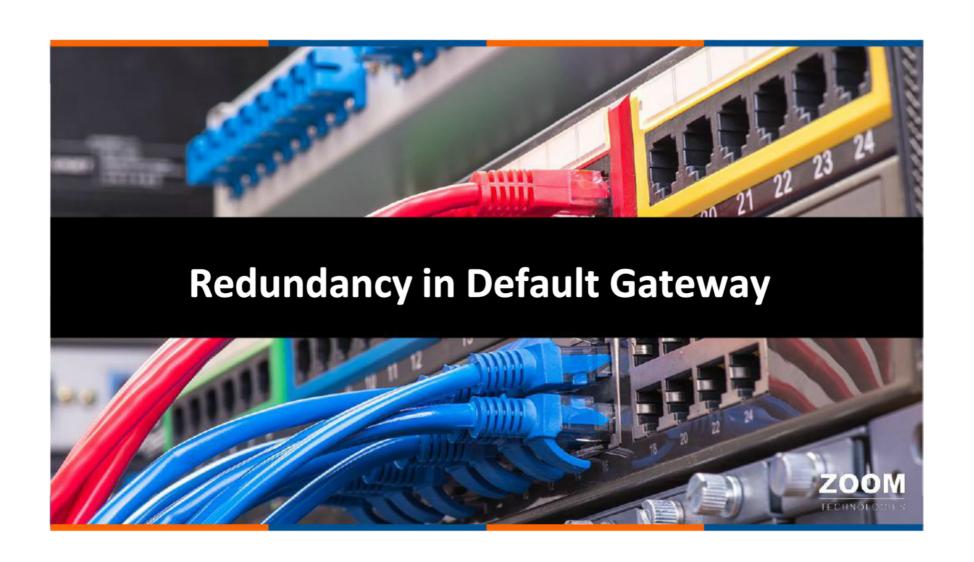


# Supervisor redundancy



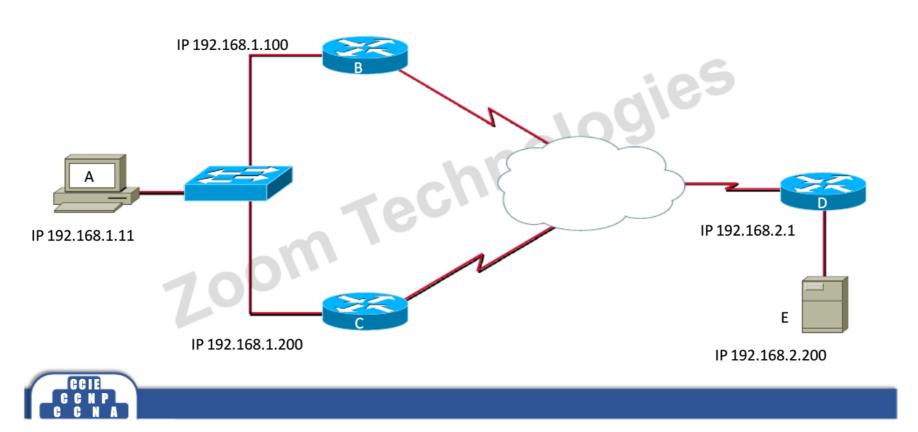


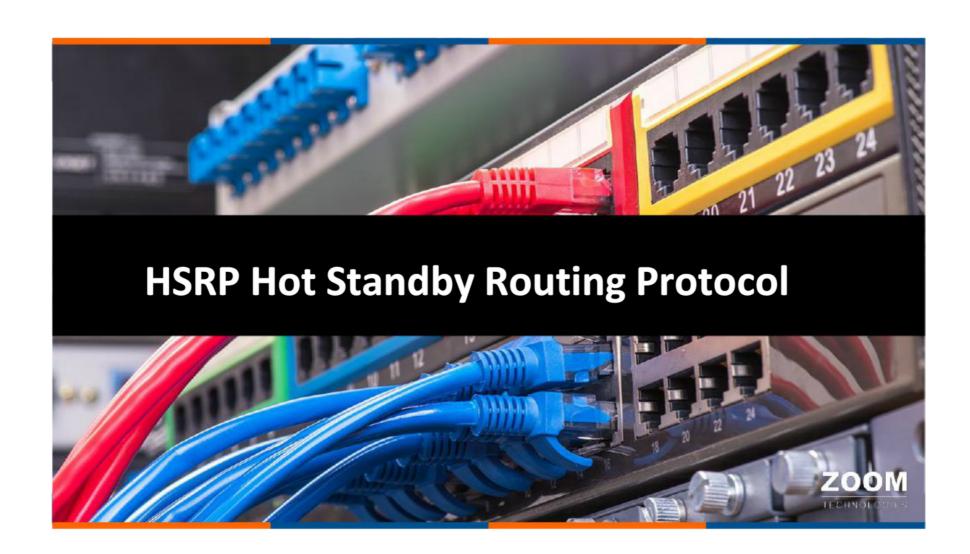




# **Problem using default Gateway**





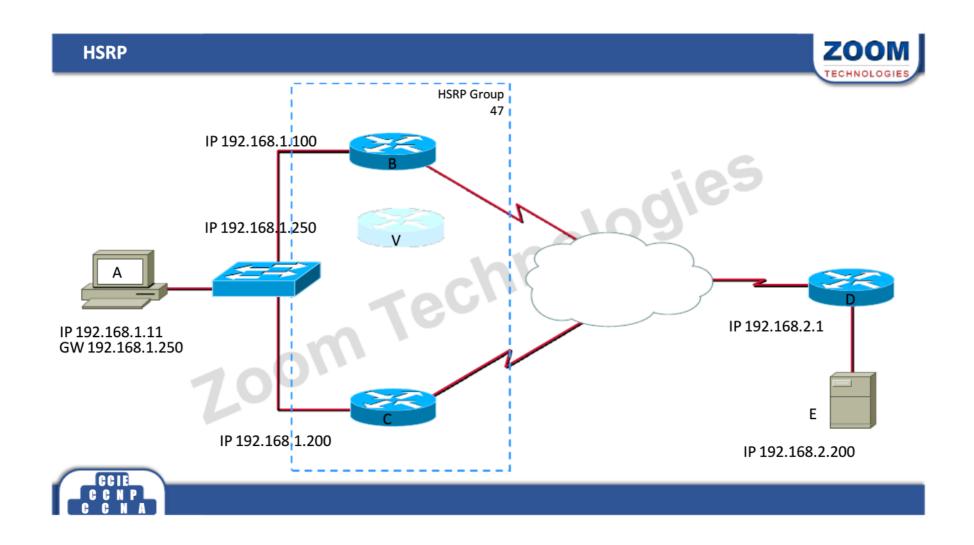


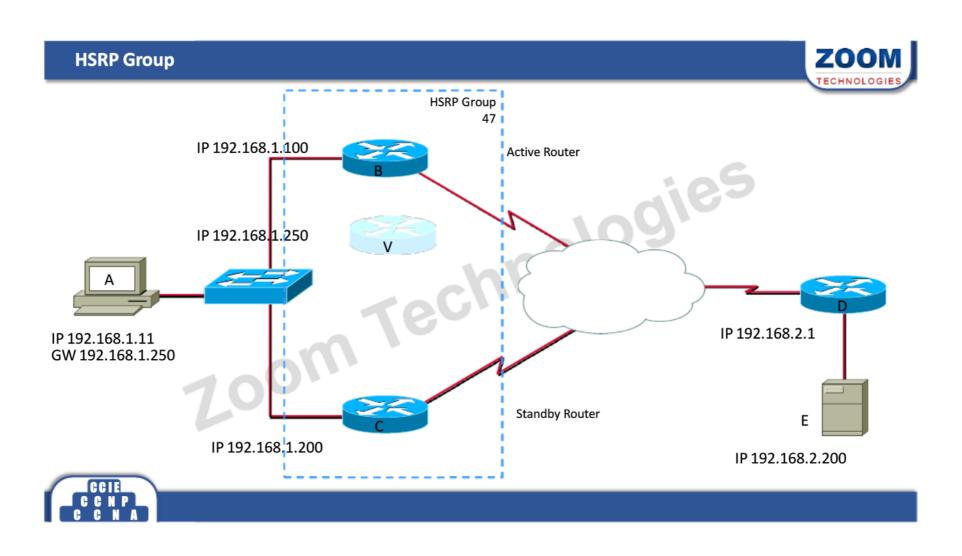
# **HSRP Hot Standby Routing Protocol**

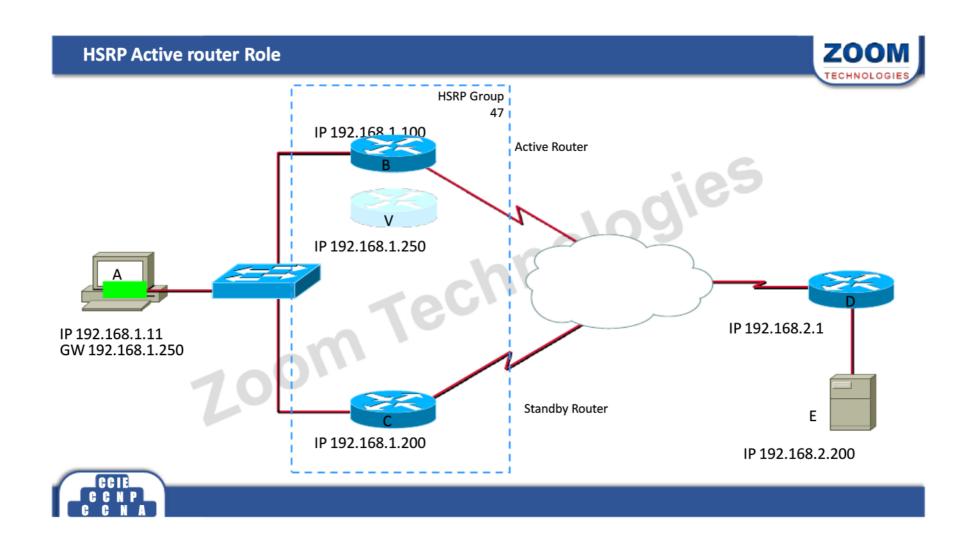


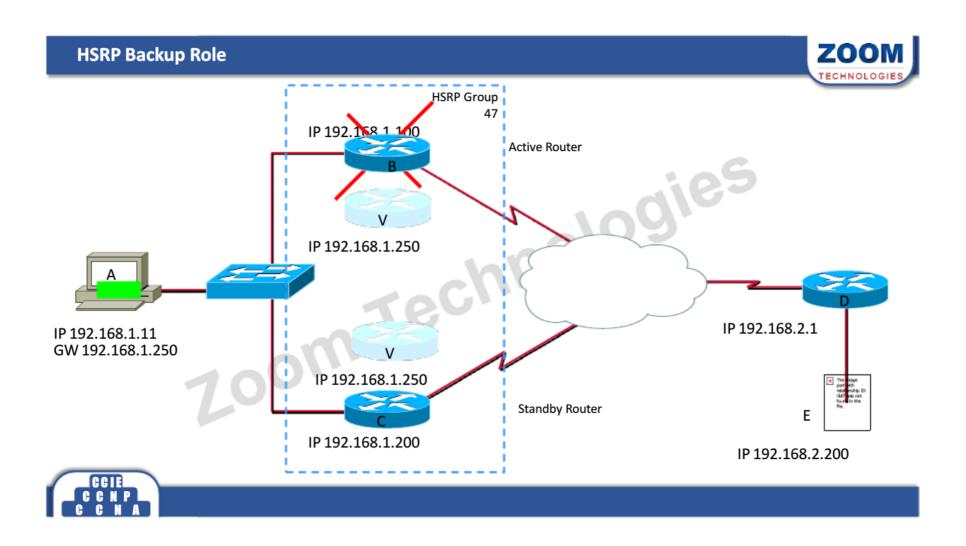
- Cisco proprietary
- Provides Router redundancy
- logies • Routers are grouped together, to work as one virtual router
- Group is identified by Group ID
  - Range 0 255 (default is 0)
  - A router can be member of multiple groups
- · Two roles of Router
  - Active Router
  - Standby Router

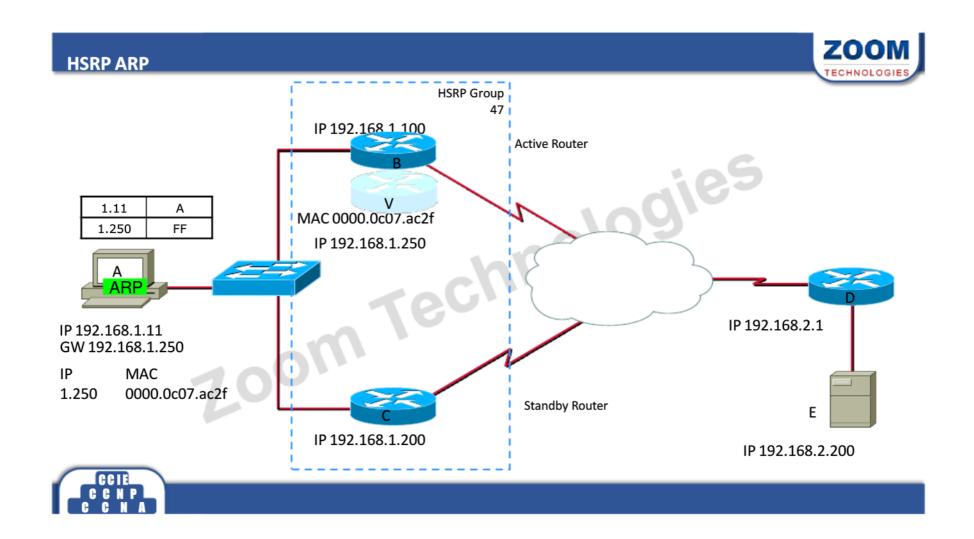












## **HSRP Elections**

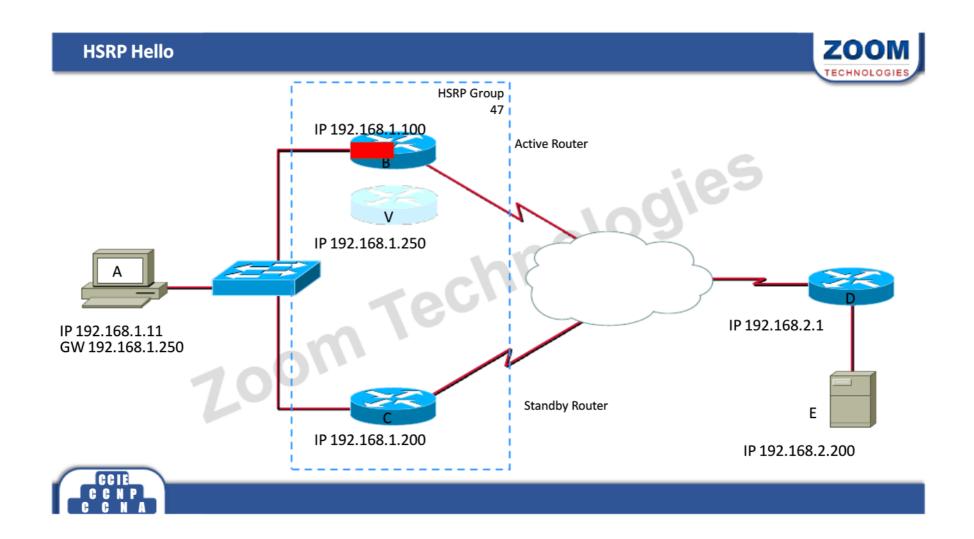


- HSRP is an Application Layer Protocol
- Uses UDP port 1985, multicast address 224.0.0.2 for hello message
- · Hello will be sent every
- HSRP Election priority

700m

коuter with highest Priority
• Router with highest Physical IP





# **HSRP Configuration**



To create and assign ip address in HSRP group

ologies Router(config-if)#standby < Group No> ip < ip add>

**Default priority is 100** 

Router with highest priority will win the elections

To change the Router priority

Router(config-if)#standby <group no> priority <pri>

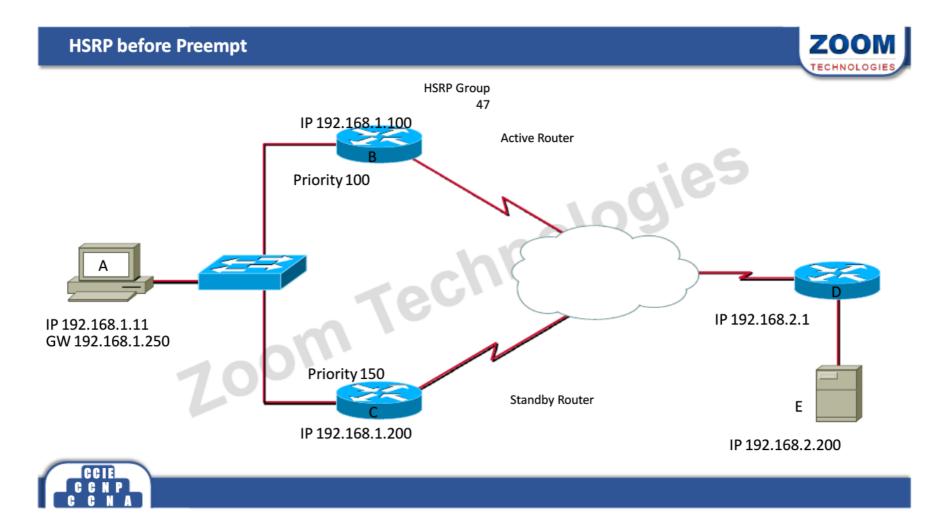


# **HSRP States**



- Initial
- Listen
- Speak
- Zoom Technologies Standby
- Active



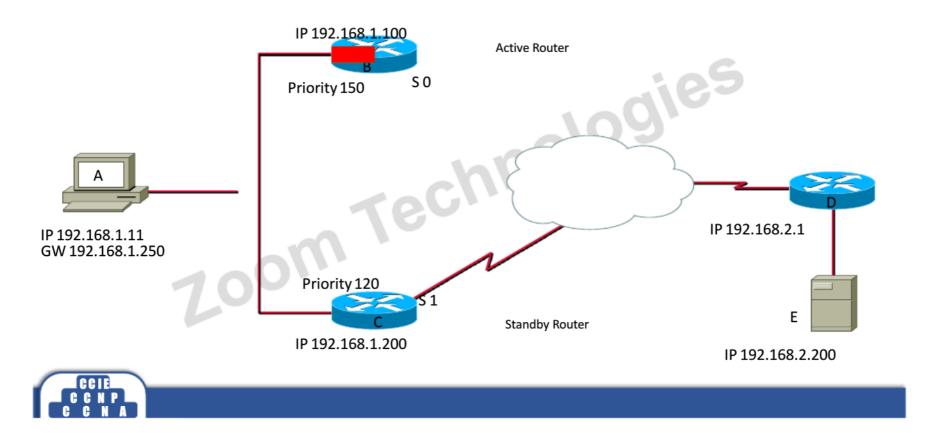


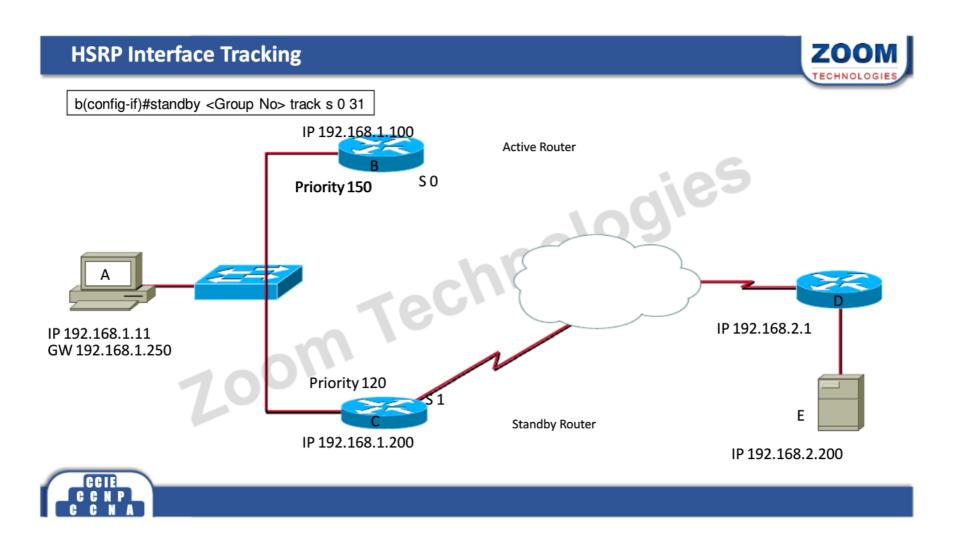
# HSRP after Preempt HSRP Group 47 IP 192.168.1.100 Standby Router Priority 100 My Priority is High1 will become Active Router IP 192.168.2.1 IP 192.168.2.200 IP 192.168.2.200 IP 192.168.2.200

# IP 192.168.1.10 Priority 150 Priority 120 IP 192.168.1.250 Priority 120 IP 192.168.1.200 IP 192.168.2.200

# **HSRP Interface Tracking**







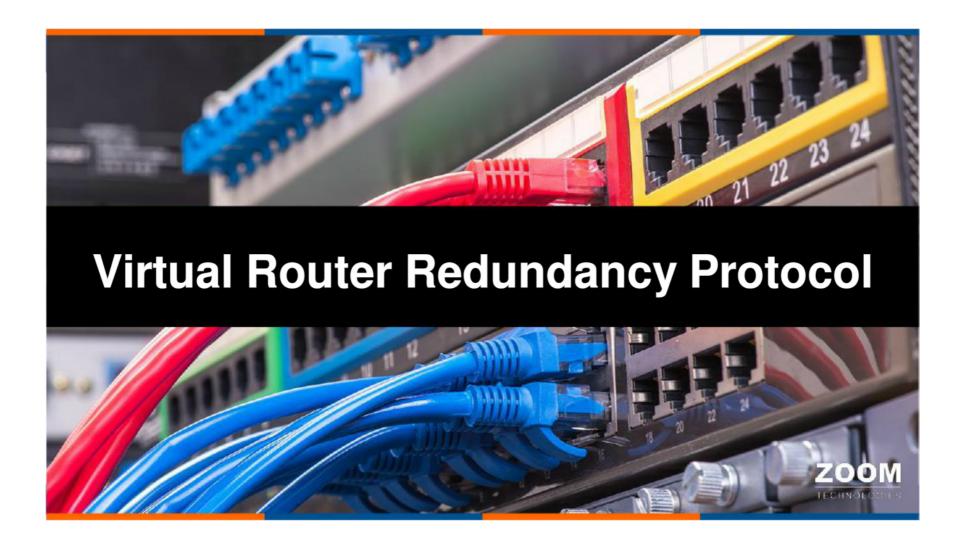


Router(config-if)#standby <G No> track <int type> <no> <Priority>

Zoom

To decrement amount of priority from HSRP
When ever interface go down
Note Preempt command is pre required on both router for this command to work





### **VRRP**



- Open Standard protocol
- Provides Router redundancy
- .er TeChnologies · Routers group together to work as one virtual router
- Group is identified by Group ID
  - Range 0 255 (default is 0)
- Group has two types of router
  - Master router
  - Backup Router



### **VRRP**



- Master Router
  - Only one master per group
  - \_roup
- Backup Router





### **VRRP Elections**

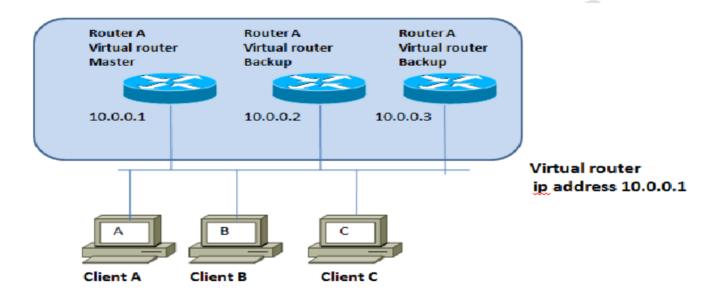


- VRRP is a Network Layer Protocol
- Uses 224.0.0.18 for hello
- · Hello will be send only by master
- Router with highest Priority
   Router with highest Phiese
- VRRP Election priority



### **VRRP**











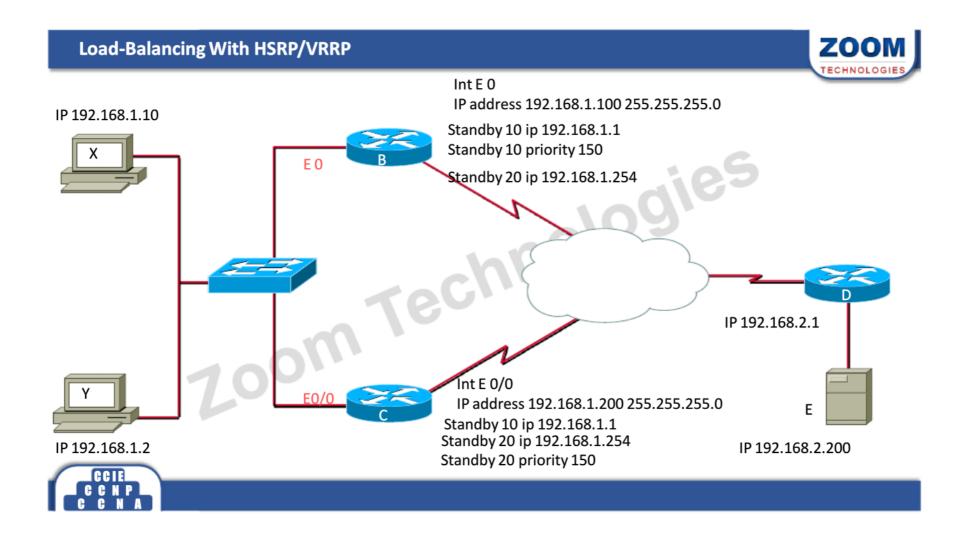
Router(config-if)#vrrp <G No> ip <IP Add>

To create VRRP Group and assign IP Address

hnologies Router(config-if)#vrrp <G No> priority <Priority>

**To Configure VRRP Priority for Election** 





# Load-Balancing With HSRP/VRRP in Multilayer Switch



Int VLAN 10

IP address 10.10.0.100 255.255.255.0

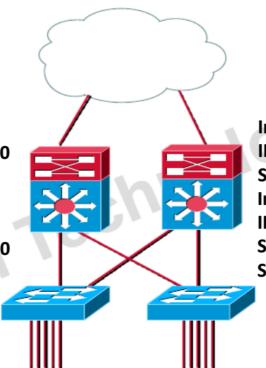
Standby 10 ip 10.10.0.1

Standby 10 priority 150

Int VLAN 20

IP address 10.20.0.100 255.255.255.0

Standby 20 ip 10.20.0. 1



Int VLAN 10
IP address 10.10.0.200 255.255.255.0
Standby 10 ip 10.10.0.1
Int VLAN 20

IP address 10.20.0.200 255.255.255.0 Standby 20 ip 10.20.0. 1 Standby 20 priority 150







### **GLBP**



- Cisco proprietary protocol
- Provides Router redundancy with load balancing
- Zoom Technologies · Routers group together to work as one virtual router
- Group is identified by Group ID
  - Range 0 1024 (default is 0)
- Group have two type of router
  - AVG
  - AVF



### **GLBP**



- AVG
- Active Virtual Gateway
- Reply for ARP coming for Virtual IP
- Divides load among AVF
- One Per group
- AVF
- Active Virtual Forwarder
- nologies Forwards user traffic coming for Virtual MAC
- There can be up to four forwarder per group oom

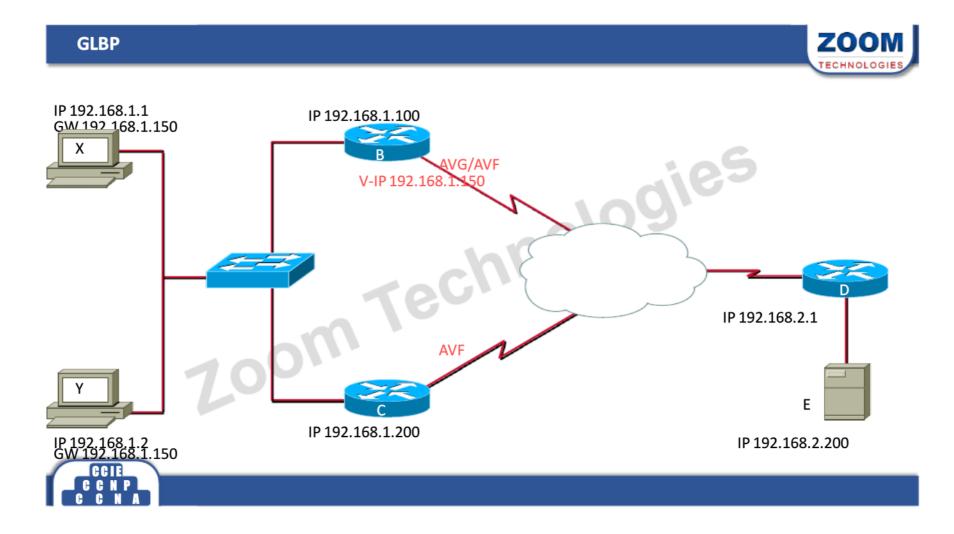


### **GLBP Elections**



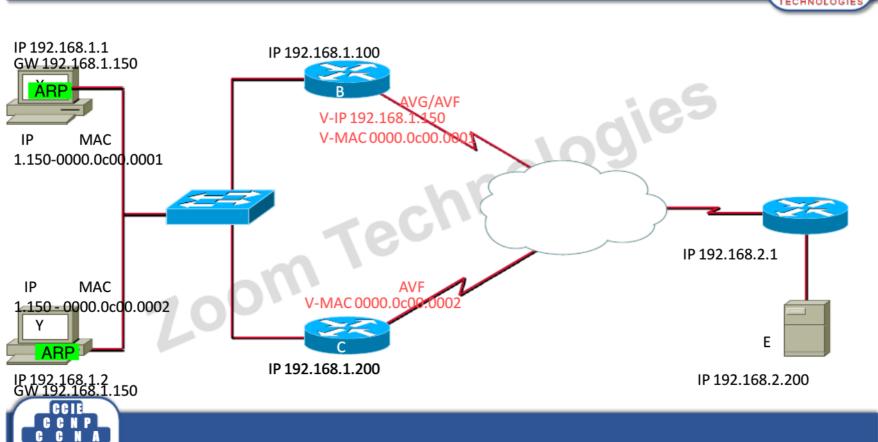
- GLBP have two elections per Group
  - Active Virtual Gateway
    - ologies • Router with Highest Priority (default 100)
    - · Router with Highest Physical IP
    - · Only one AVG Per group
    - Election are non-preemptive
  - Active Virtual Forwarder
    - Router with Highest weight (default 100)
    - · Router with Highest Physical IP
    - · Up to four AVF Per group
    - Election are preemptive

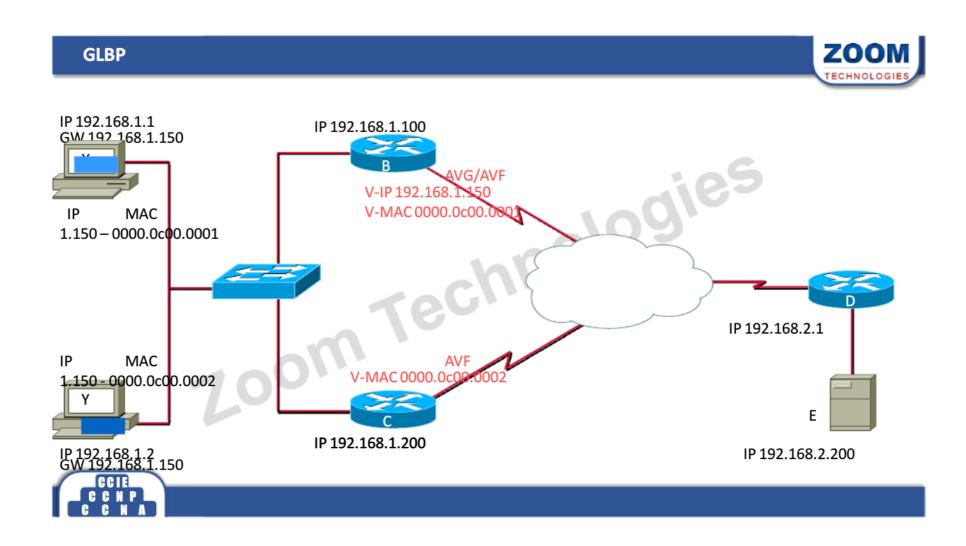




# **GLBP**





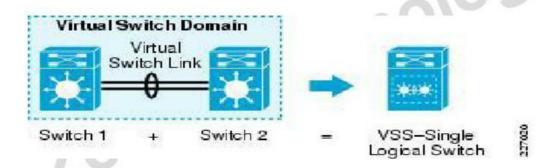


# **GLBP** ZOOM TECHNOLOGIES IP 192.168.1.100 IP 192.168.1.1 GW 192 168.1.150 V-MAC 0000.0c00.0 ΙP MAC 1.150 - 0000.0c 00.0001 IP 192.168.2.1 IΡ MAC /-MAC 0000.0c0 1.150 - 0000.0c00.0002 00.0001 Ε IP 192.168.1.200 IP 192.168.1.2 GW 192.168.1.150 IP 192.168.2.200

# **VSS**



- The Virtual Switching System (VSS) allows two Cisco Catalyst 6500 or 4500 to combine together as one mega switch
- Other devices will see the VSS configured 6500 as a single device
- Two switches will be combined by using a special link called a Virtual Switch Link( VSL) .

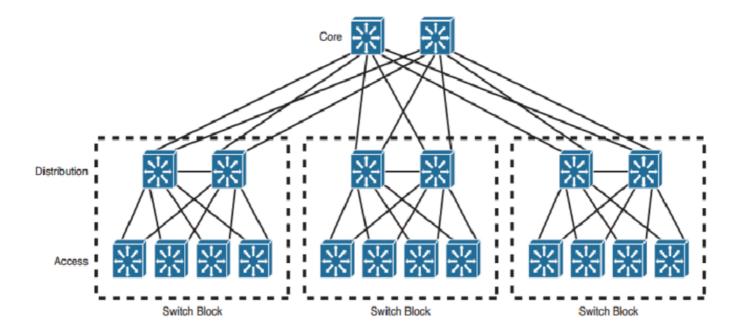






# **Without VSS**

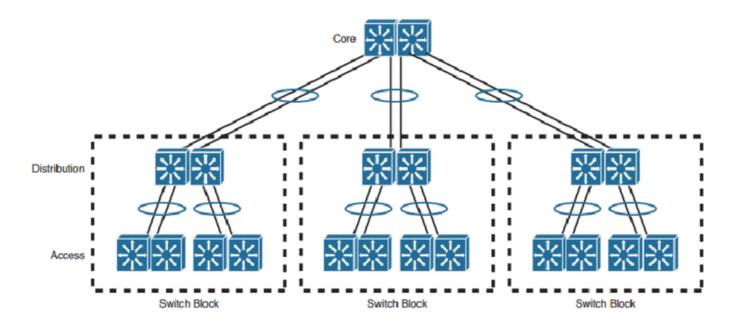






# With VSS











# **Recommended Switch Security**



- Configure Secure Passwords
- Configure basic ACLs
- ners Secure physical access to the console
- Secure access to VTYs
- Configure system warning banners
- Disable unneeded services 7.00m
- SSH







- Authentication
  - Verifies a user's identify
- Authorization
- ogies - Specifies the permitted tasks for the user
- Accounting
  - Provides billing, auditing and monitoring



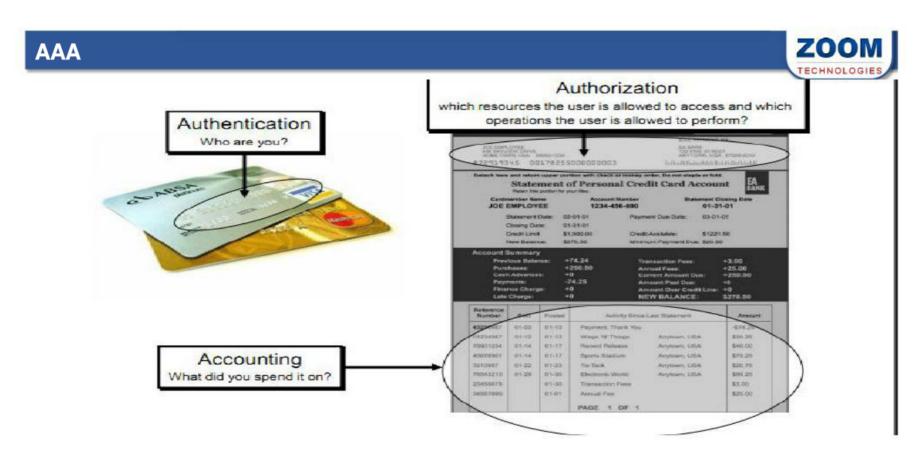
## **AAA in a Nutshell**



- Authentication provides the method of identifying users. The most common method of authentication is username/password.
- Authorization provides a method of controlling access to what a user can do. Authorization is usually tied to a policy, profile or group.
- Accounting provides a method for collecting and sending security server information used for billing, auditing, and reporting.
  - Accounting collects data as to what a user did once logged in.









# AAA



- Zoom Technologies AAA can be implemented with the help of two protocols
- **Radius**
- Tacacs+



# To enable AAA



- Switch(conf)#aaa new-model
- ologies Switch(conf)#aaa authentication login default group radius
- Switch(conf)#radius-server host 192.168.0.1 key zoom123
- Switch(conf)#line vty 0 4
- Switch(conf-line)#login authentication default

oom



# **Switch Attack Categories**



MAC Flooding Attack

MAC Flooding attack is a type of attack where switch port will receive large number of Frames with Fake MAC addresses.

VLAN Hopping Attack

VLAN hopping (virtual local area network hopping) is a method of attacking a network by sending packets to a port that is not normally accessible from a given end system.

Spoofing Attacks

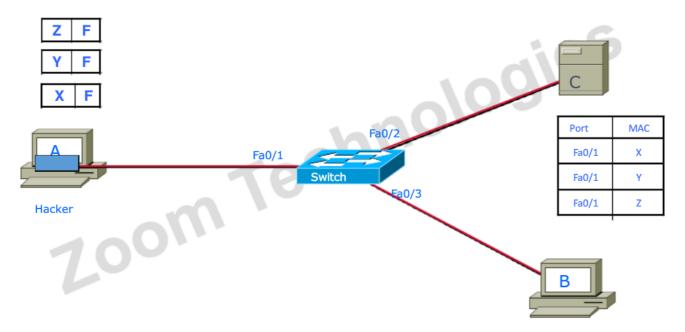
Switch spoofing can occur when the switch port an attacker connects to is either in trunking mode or in DTP auto-negotiation mode





# **MAC Flooding Attacks**

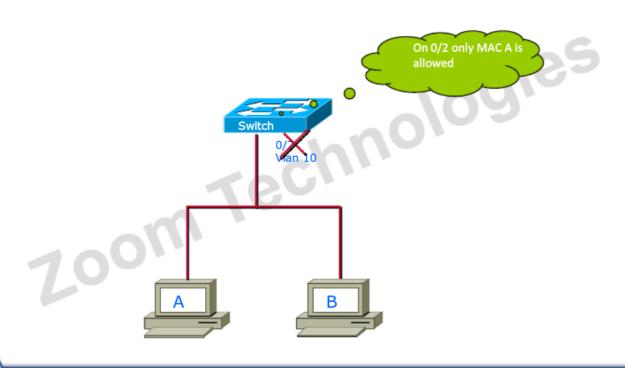






# **Network Access Port Security**









# **Network Access Port Security**





Switch(c)#interface fa 0/2

nnologies urit: Switch(c-if)#switchport port-security

Switch(c-if)#switchport port-security max 1

Switch(c-if)#switchport port-security mac-address

0000.0000.000a

Switch(c-if)# switchport port-security violation <shutdown | protect | restrict>



# **Verification of port security**



# Switch#show port-security

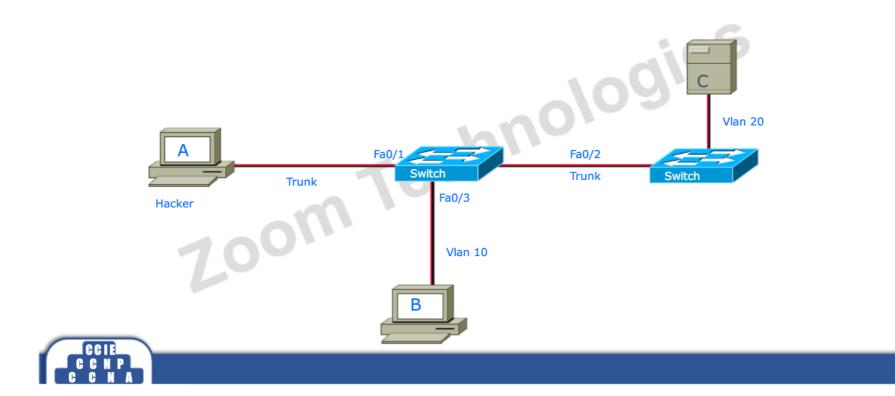
Switch#show	port-security			1.5
				dies
Switch#show port-security				
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa5/1	11	11	0	Shutdown
Fa5/5	15	5	0	Restrict
Fa5/11	5	4	0	Protect
Total Addresses in System: 21				
Max Addresses limit in System: 128				





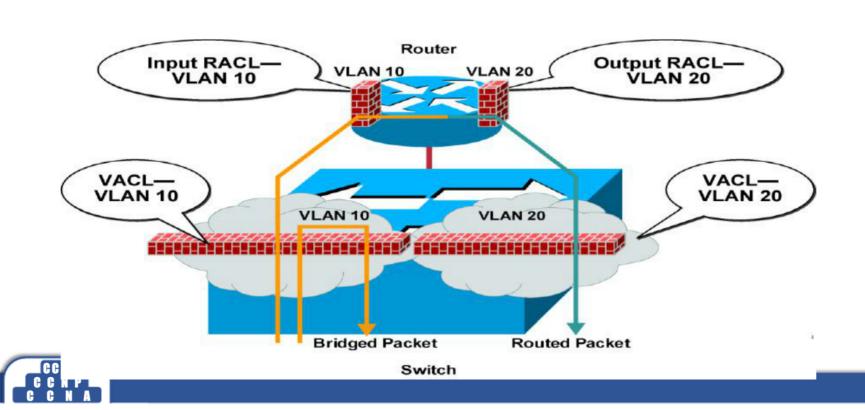
# **VLAN Hopping**





# Type of ACLS







#### **VLAN Access List**



- Used to filter traffic within one Vlan
- Zoom Technologies It is configured using access-map
- It is implemented per VLAN
- It can filter the traffic base on MAC
- Extended MAC list is Required



## Vlan Access-list



#### **Creating Extended MAC ACCESS list**

s(c)#mac access-list extended zoom

s(c-ext-macl)#permit 0000.0000.000a 0000.0000.0000 0000.0000.000b 0000.0000.0000 hnologi

#### **Creating Access-map**

s(c)#vlan access-map V10 10

s(c-access-map)#match mac address zoom

s(c-access-map)#action drop|forward

#### **Implementing**

s(c)#vlan filter v10 vlan-list 10

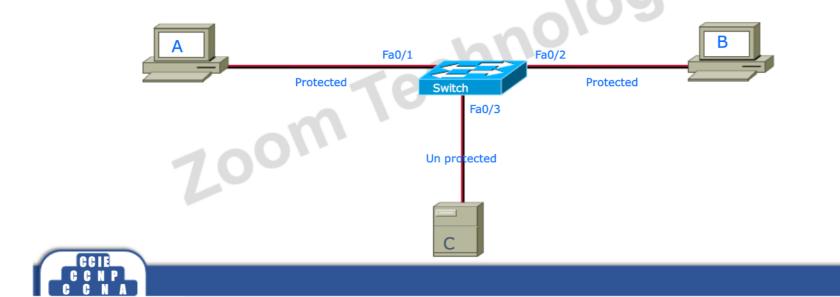




#### **Switchport Protected**



Protected port is a feature on Cisco switches that is used to prevent interfaces are communicating with each other.



#### **DHCP Spoofing**



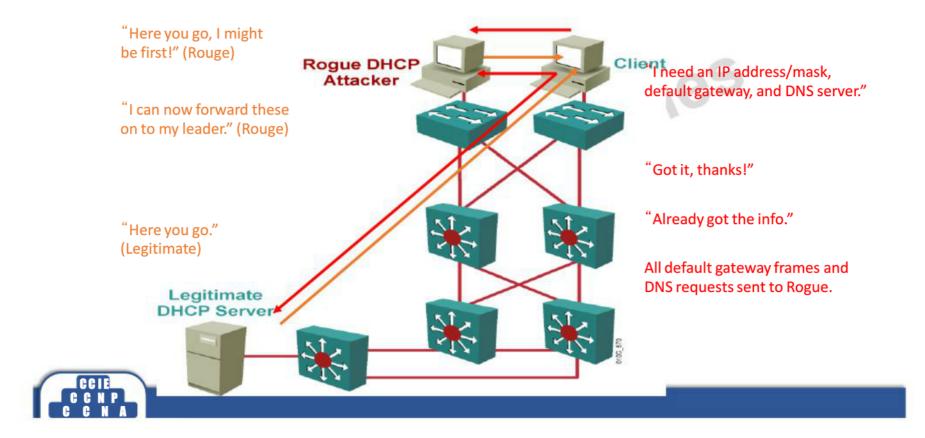
- DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients.
- The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".
- The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.





# **DHCP Spoofing Attacks**

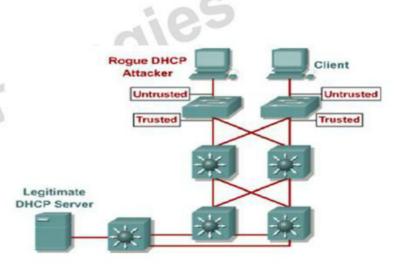




## **DHCP Snooping**



- Cisco Catalyst feature that determines which switch ports can respond to DHCP requests.
- Trusted ports can source all DHCP messages
   while untrusted ports can source requests only.
   Should not send any DHCP server responses,
   such as DHCPOFFER, DHCPACK, or DHCPNAK
- If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down.

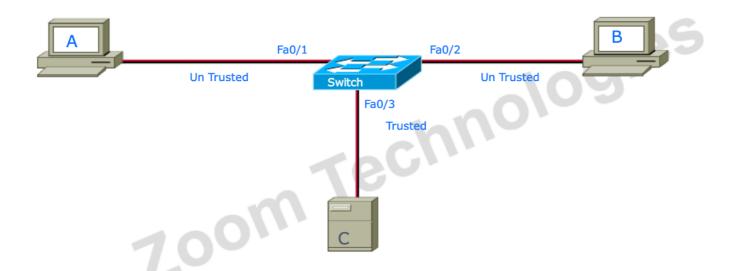






# **DHCP Snooping**







## **DHCP Snooping Configuration**



Switch(config)#ip dhcp snooping

Switch (config) #ip dhcp snooping

Enable DHCP snooping globally

Switch (config) #ip dhcp snooping information option

Enable DHCP Option 82 data insertion

Switch(config-if) #ip dhcp snooping trust

· Configure a trusted interface

Switch (config) #ip dhcp snooping vlan number [number]

Enable DHCP snooping on your VLANs





## **DHCP Snooping Configuration**



Switch(config)#ip dhcp snooping (enable dhcp snooping globally)

Switch(config-if)#ip dhcp snooping trust (configure trusted interface)

hnologies Switch(config)#ip dhcp snooping vlan number[number] ( enable dhcp on vlans)



#### **Verification of DHCP Snooping**



# Switch#show ip dhcp snooping

Verify the DHCP snooping configuration

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
   10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface
                   Trusted
                                   Rate limit (pps)
FastEthernet2/1
                   yes
                                   none
                  yes
FastEthernet2/2
                                   none
FastEthernet3/1
                                   20
                   no
Switch#
```





# **Dynamic ARP Spoofing**

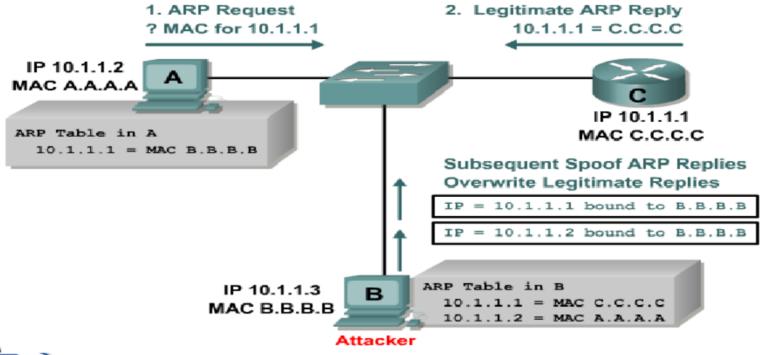


- ARP Spoofing is a type of attack where attacker sends fake arp messages to implement man in the middle attacks.
- Dynamic ARP inspection prevents ARP spoofing by checking all ARP requests and ARP replies.
- DHCP snooping must be configured before enabling DAI.
- Dynamic ARP Inspection uses DHCP snooping binding table to protect against ARP spoofing attacks.
- The switch checks the MAC to IP binding in the ARP reply with the DHCP snooping database.
- Drops invalid ARP replies.



# **ARP Spoofing**







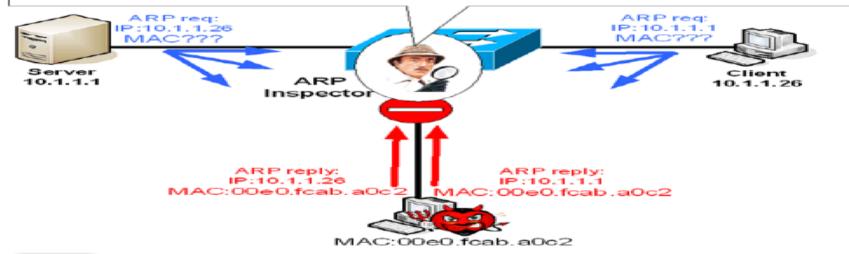


# **Dynamic ARP Inspection**



#### DHCPSBDB:

IP Addr	VLAN	MAC	LeaseTime	Port	Checksum
10.1.1.1	22	00e0.fc5a.0e1b	3EBE2881	Gi1/1	e5e1e733
10.1.1.26	22	00e0.2245.3c4c	34ABE45E	Fe3/8	a111f69b





# **Dynamic ARP Inspection**

7.00m



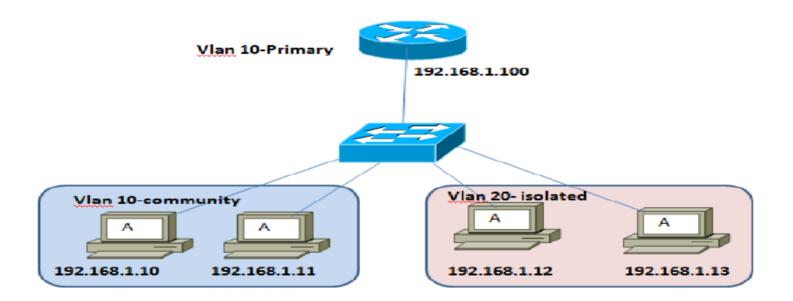
Configure DAI on switch:

gies Switch(config)#ip arp inspection vlan < vlan-range>











# **Private Vlan**



- Private vlan = vlan inside of vlan
- Private-vlans mainly used by service provider networks.
- · Private vlan is the combination of primary and secondary vlan.
- Primary vlan's are same as normal vlans





# **Private Vlan**



### Secondary vlans will work in two modes

- Community: Ports belong to this vlan will communicate with each other
- Isolated: Ports belong to this vlan will not communicate with each other

Port assigned to Private vlan will work in two modes

- Host: belongs to one private vlan
- Promiscuous : belongs to multiple private vlan



#### **Storm Control**



- Storm control is the method to control the traffic on particular interface.
- There are 3 kinds of traffic you can manage on the interface

Loom

- Unicast
- Multicast
- Broadcast



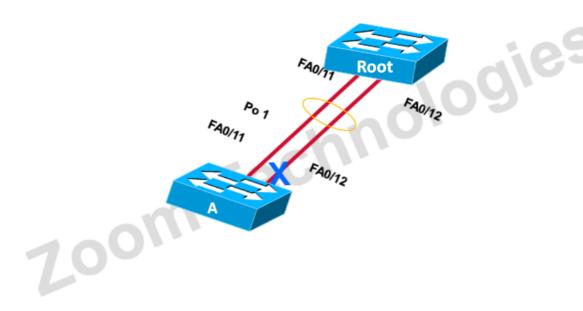






**Switch Path** 









### **Ether Channel**



- · Logical aggregation of similar links
- Viewed as one logical port
- · Switch-level load balancing
- Redundancy
- · Can be used between switch to switch, Router, firewall and server

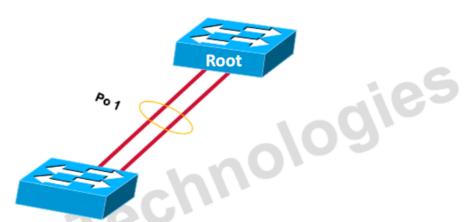
#### Note:

Only similar physical link with same configuration can be aggregated. Max 8 similar links can be bundled (depend on Hardware)



#### **Ether Channel**





- · Ether channel configuration can be done in two ways
  - Static (always On mode)
  - Dynamic (using PAgP, LACP)

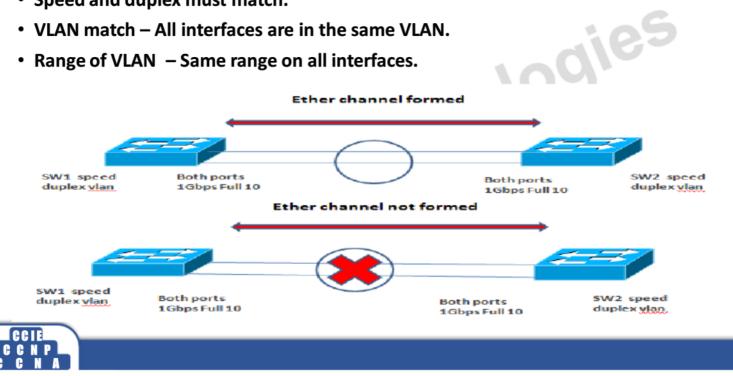




## **Configuring EtherChannel**



- EtherChannel must be supported.
- Speed and duplex must match.
- VLAN match All interfaces are in the same VLAN.
- Range of VLAN Same range on all interfaces.



# **Port and Link Aggregation**



- Port Aggregation Protocol (PAgP)
  - Cisco-proprietary protocol
  - , rassive PAgP Have two Mode Desirable / Auto
- Link Aggregation Control Protocol (LACP)
  - Defined in IEEE 802.3ad
  - LACP have two mode Active / Passive





# **Configuring PAgP**



Switch(config) #interface type <mod/num>

Switch(config-if)#channel-protocol <pagp/lacp>

Configures the interface in a port-channel and specifies the PAgP mode



## **Verifying EtherChannel**



Switch#show running-config interface port-channel num

• Displays port-channel information

Switch#show running-config interface interface x/y

Displays interface information

#### Switch#show run interface port-channel 1

Building configuration...
Current configuration:
!
interface Port-channel1
no ip address
no ip directed-broadcast
end

#### Switch#show run interface gig 0/9

Building configuration...

Current configuration:
!
interface GigabitEthernet 0/9
no ip address
channel-group 1 mode desirable
end





#### **Verifying EtherChannel (Cont.)**



Switch#show etherchannel num port-channel

Displays port-channel information after configuration

```
Switch#show etherchannel 1 port-channel
Port-channels in the group:
Port-channel: Po1
Age of the Port-channel = 01d:01h:31m:38s
Logical slot/port = 1/0 Number of
                   = 1/0 Number of ports = 2
= 0x00020001 HotStandBy port = null
                   = Port-channel Ag-Inuse
Port state
Ports in the Port-channel:
Index Load
               Port EC state
-----+-----
       00
               Gi0/9 desirable-sl
            Gi0/10 desirable-sl
                               00d:20h:04m:38s
                                                    Gi0/9
Time since last port bundled:
Time since last port Un-bundled: 00d:21h:17m:20s
                                                    Gi0/10
```

#### **Ether Channel Load balancing**

CCIE



- Data sent across an Ether Channel is not load-balanced equally among all interfaces.
- Ether Channel utilizes a load-balancing algorithm, which can be based on several forms of criteria, including:





#### **Ether Channel Load balancing**



- Source IP Address (src-ip)
- Destination IP Address (dst-ip)
- Both Source and Destination IP (src-dst-ip)
- Source MAC address (src-mac)
- Destination MAC address (dst-mac)
- hnologies • Both Source and Destination MAC (src-dst-mac)
- Source TCP/UDP port number (src-port)
- Destination TCP/UDP port number (dst-port)
- Both Source and Destination port number (src-dst-port)



# **Configuring EtherChannel Load Balancing**



7.00m 1echnolo Switch(config) #port-channel load-balance type

Configures EtherChannel load balancing









#### **Simple Network Management Protocol**



- ..d conf SNMP is a protocol used for network management, i.e. to monitor and configure devices on IP networks.
- SNMP works in Application Layer (Layer 7)
- SNMP uses UDP
- SNMP uses port No. 161





# **SNMP Components**



- SNMP MANAGER
- SNMP AGENT

# Zoom Technologies



#### **SNMP Functions**



- Monitor Network Performance
- Audit Network Usage
- Detect Network Faults
- Detect Inappropriate access
- · Configure remote devices





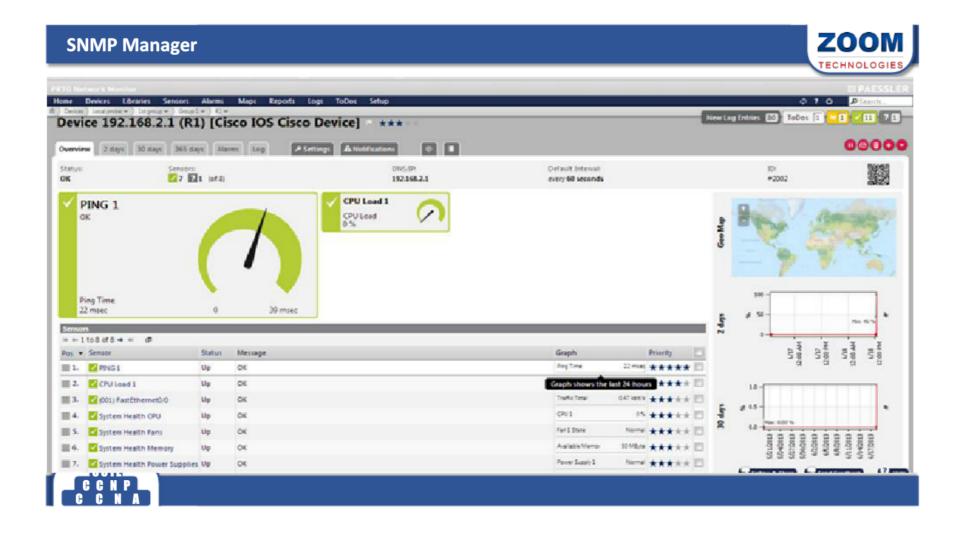


#### **SNMP Manager**



- · SNMP Manager is a software that collects information from network devices.
- work. SNMP Manager is installed on a workstation or PC to manage the network. We call this PC or Workstation as Network Management System.
- EX: PRTG, Cisco Prime, Solar Winds







#### **SNMP Agent**

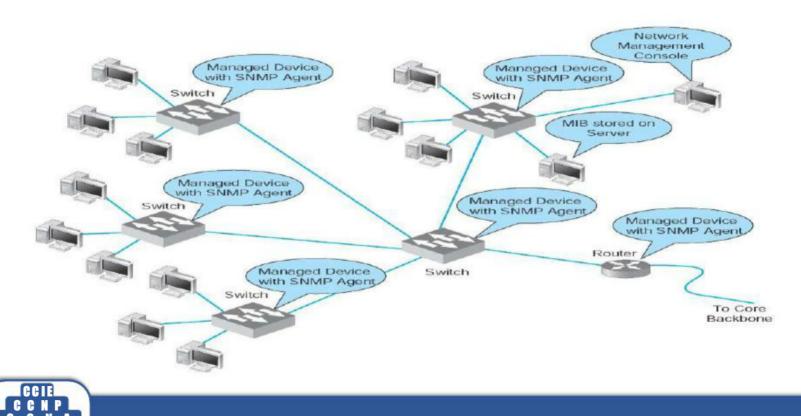


- SNMP Agent is the software that is installed on network managed devices such as Router (or) Switch (or) Server (or) PC.
- Agents collects information and then sends it to monitoring station whenever it is asked.
- Agents are usually built into your network hardware and software. They simply need to be enabled.



#### **SNMP Agent**







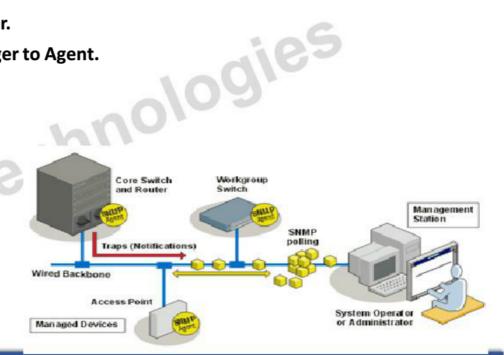
#### **Polling**



- In Polling method, SNMP Manager continuously asks a network device to report the statistics of device.
- Example: Interface Status of Router.

Zoom

Request is sent from SNMP Manager to Agent.

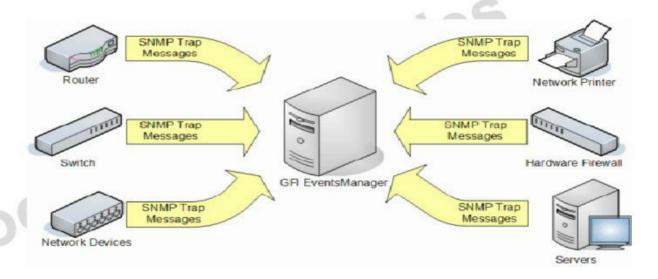




#### **TRAP**



• Trap is where device reports an event to NMS, for example whenever High CPU utilization or High Memory Utilization or Link Down is detected.







#### **SNMP Modes**



- Read Only Mode:
  - · used to retrieve information from network devices.
- Read Write Mode
  - Les as well Used to retrieve the information from network devices as well as to configure the devices.



#### **Management Information Base**



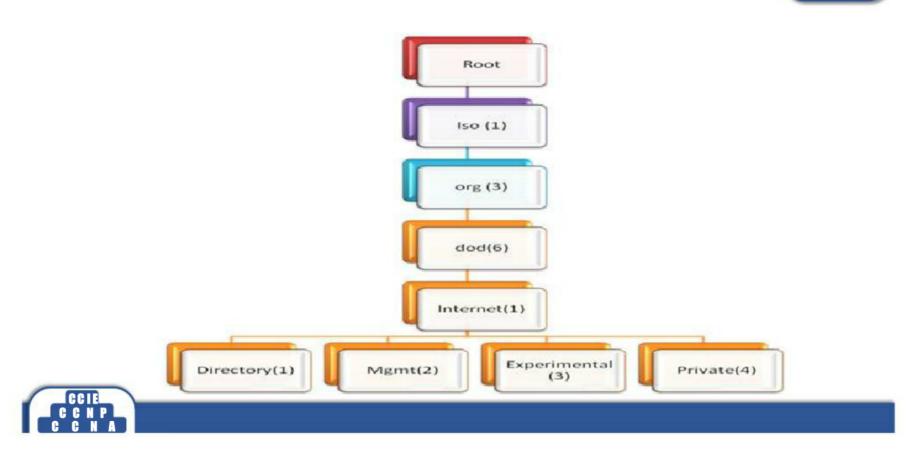
- Management Information Base (MIB) contains collection of information which is Object Identifier
   Read/Only or Read/Write Type organized hierarchically.
- Management Information Base contains-





## **Object ID structure**





#### **SNMP Versions**



- Zoom Technologies SNMP V1
- SNMP V2
- SNMP V3



#### **SNMP Version 1**



dies

- It is the initial version of SNMP Protocol.
- · Data is sent in the clear text format.
- It should be used in private networks only.
- They use the community string to authenticate the peers.
- Uses Get Request to retrieve the information about particular object. ..atio



#### **SNMP Version 2**



- SNMP Version 2 is the enhanced version of SNMP.
- Improved Error Handling and Error Reporting
- Get Bulk Request command is used to retrieve the information.

   It also uses community string to a second community string t
- היים e the peers. It also uses community string to authenticate the peers.





#### **SNMP Version 3**



- Zoom Technologies Provides secure access using authentication and encryption.
- Consumes more CPU memory compared to other versions.
- It defines 3 Security levels.



#### **SNMP** configuration



#### **Requirement:**

- Configure SNMP on your router or switch
- Router(config)#snmp-server enable traps
- gies Router (config)#snmp-server host 192.168.0.50 version 2c public
- Router(config)#snmp-server location Hyderabad
- Router(config)#snmp-server contact zoomgroups oom







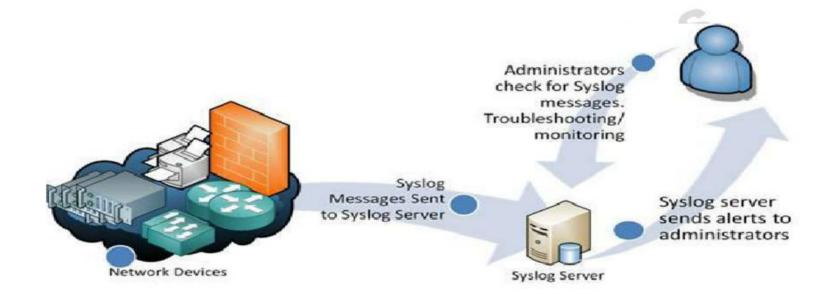
#### What is Syslog



- · Syslog is a standard for message logging.
- Syslog is a network management protocol which allows network devices to report error and notification messages either locally (or) to a remote syslog server.
- Syslog messages are sent in plain text using UDP port No. 514.









## **Syslog Components**



- Syslog Server
  - A host that accepts and processes log messages from 1 or more syslog clients.
- Syslog Client
  - A host that generates log messages and forwards them to a syslog server. .uem
  - Ex: Router, switch, firewall, modem





Facility Mnemonic

%SYS-5-CONFIG\_I: Configured from console by console Severity 200m

odies



# **Configure syslog**



#### Requirement:

- aging 7.000 • Configure syslog server to store the messages in a server.
- R1(config)# logging on
- R1(config)#logging 192.168.0.50
- R1(config)#logging trap i4
- Verification:
- R1#show logging







# **Telnet vs SSH**



Telnet	SSH		
Port No. 23	Port No. 22		
Uses TCP	Uses TCP		
Not Secured	Secured		
Works in Application Layer (Layer 7)	Works in Application Layer (Layer 7)		







	ies
Telnet	SSH
➤ Telnet is a protocol which allows you to access any device remotely.	➤ SSH is a protocol which allows you to access any remote device securely
➤ It sends the data in Clear-Text format.	➤ It sends the data in Encrypted format.
7.00M	

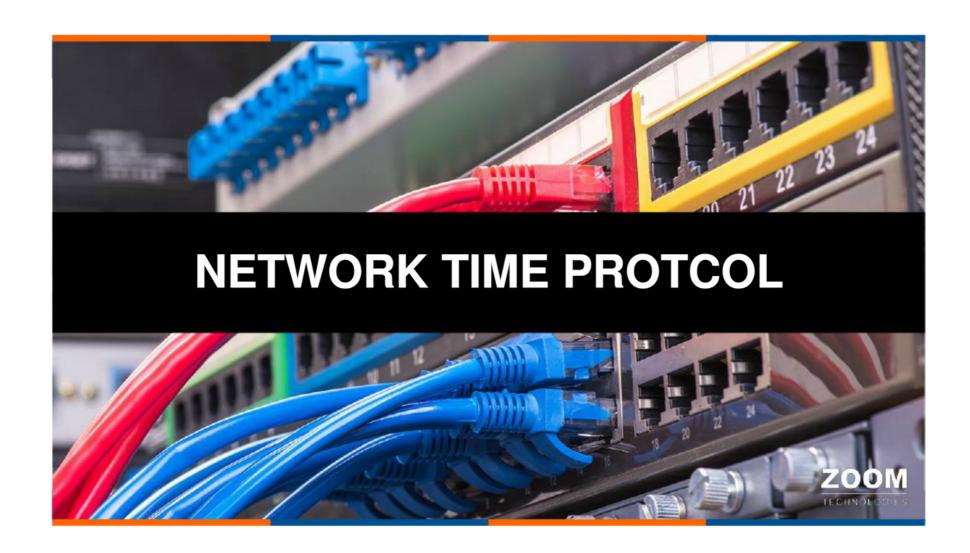


# **SSH** configuration



- Requirement:
- Configure SSH on SW1.
- SW1(config)#hostname ssh
- ;chnologie<sup>s</sup> • SW1(config)#ip domain-name zoom.com
- SW1(config)#crypto key generate rsa
- SW1(config)# line vty 0 4
- SW1(config-line)# transport input ssh
- SW1(config-line)#login local
- SW1(config-line)#passwordzoom
- SW1(config-line)#exit
- Verification:
- SW1#show ip ssh





#### **NTP**



- Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) is the global standard for time representation. Zoom Technologies
- Most of the network enabled devices have two clock sources





#### **NTP**



- NTP provides accurate timing services to each and every network enabled device.
- Zoom Technologies It provides automatic synchronization of device clock with one or more time servers which provide accurate time.
- NTP uses UDP port number 123.



#### **Stratum**



- NTP servers are described in terms of stratum
- (hierarchical levels).
- · Stratum defines the accuracy of the clock. The most accurate clock is referred as reference clock or stratum 0 clock.
- a nigher t · Each NTP server assigned a stratum one higher than the upstream device with which is synchronized.







- hnologies • NTP can be disabled on a particular interface
  - Router(config-if)# ntp disable
- Configure NTP in Cisco Device-
- R(config)# ntp source <interface>
- R(config)# ntp authenticate
- R(config)# ntp authentication-key < number > md5 < key >
- R(config)# ntp trusted-key <key-number>
- R(config)# ntp server <ip-address> key <key-id>





#### **IP SLA**



- IP SLA is a technology from Cisco that actively monitors traffic to measure the performance of the network.
- ...g paramete Performance of the network can be measured by using following parameters
  - Jitter
  - Latency
  - Packet Loss



#### **Configure SLA**



- Configure SLA on Router
- R(config)# ip route 0.0.0.0 0.0.0.0 s0/0 Track1
- R(config)# ip route 0.0.0.0 0.0.0.0 s0/1 20
- R(config)# track 1 rtr 1
- R(config)# ip sla 1
- nologies R(config)# icmp-echo 30.1.0.1 < Destination IP>
- R(config)# frequency 5
- R(config)# exit
- R(config)# ip sla schedule 1 start-time now life forever
- R(config)# end
- R# Show IP SLA Statistic



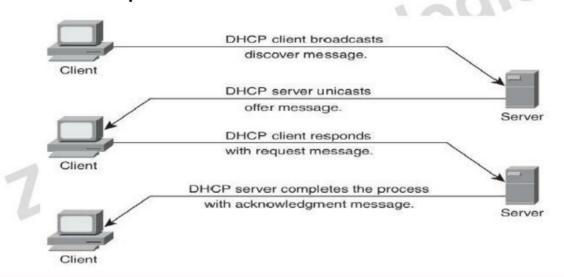




# DHCPV4



- DHCP is a dynamic way of assigning network configuration parameters to clients.
- DHCP uses port number 67 and 68.
- DHCP uses DORA process.
- DHCP uses broadcast packets.





#### Configuring a router as a DHCP server



- Requirement:
- Assign IP address on Lan interface of the R1 router.

   R1(conf)# interface fastethernet 0/0

   R1(conf-if)# ip address 192 168 5 1 355 355

- R1(conf-if)# no shutdown
- R1(config)#ip dhcp pool zoom
- R1(dhcp-config)#network 192.168.5.0 255.255.255.0
- R1(dhcp-config)#default-router 192.168.5.1
- R1(dhcp-config)#dns-server 192.168.5.1
- R1(dhcp-config)#end





- R1(config)# ip dhcp excluded-address 192.168.5.1
- Zoom Technologies R1(config)#ip dhcp pool zoom
- R1(dhcp-config)#lease 1
- Verification:
- R1#show ip dhcp binding







### **DHCP Relay Agent**



- DHCP Relay Agent forwards DHCP messages between DHCP clients and DHCP Servers which reside on different IP network.
- By default router will not forward broadcasts, DHCP relay agent will convert broadcast into unicast packets.







Router(config-if)# ip helper-address < DHCP server IP address>





#### **SPAN and RSPAN**



- Switched Port Analyzer (SPAN) is also called Port Monitoring; used for Network Analysis.
- SPAN allows you to select one or more ports for analysis.
- SPAN is used to monitor devices on only one switch.
- Remote SPAN is used to monitor devices on more than one switch.



#### **SPAN Configuration**



- Switch(config)#monitor session 1 source interface fa0/2
- Switch(config)#monitor session 1 destination interface fa0/1







### **RSPAN Configuration**



gies

SW1(config)#vlan 100

SW1(config-vlan)#remote-span

SW2(config)#vlan 100

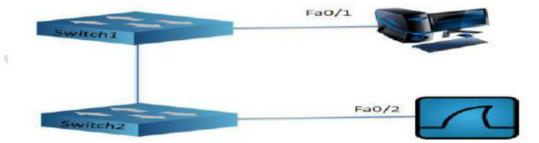
SW2(config-vlan)#remote-span

SW1(config)#monitor session 1 source interface fastEthernet 0/1

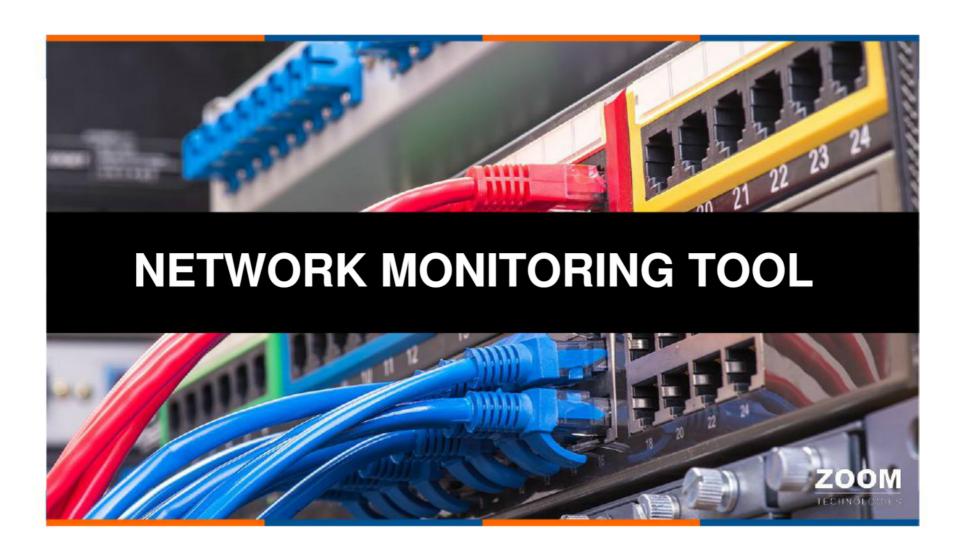
SW1(config)#monitor session 1 destination remote vlan 100

SW2(config)#monitor session 1 source remote vlan 100

SW2(config)#monitor session 1 destination interface fastEthernet 0/2









## Agenda



- **What is Network Monitoring**
- Apout PRTG.
  Some practical things



## What is Network Monitoring?









- Network Monitoring means continuously monitor a networks Techni performance.
- Bandwidth utilization,
- · Packet loss,
- Latency(Delay)
- availability and uptime



#### Why Need To Monitor Network.?



- Optimize network reliability
- Visualize network topology
- Stay in touch with your network
- Understand capacity utilization
- Troubleshoot device and traffic issues
- · Save time in network administration
- Track trends
- · Improve the bottom line



chnologies

## **Function of network monitoring**



- Administrators need to know what's happening on their networks at all times mologies
- Track Network performance
- Diagnose problems quickly.
- Keep Record of historical information
- Intelligent notifications (via SMS and mail)
- Save Time & Money.... oom



#### **About Network Monitoring Tool?**



- There are so many network monitoring tools available on global platform.
- Some of them are free and some are paid.
- Free tools have some limitations, It can't give us deep performance information about network.





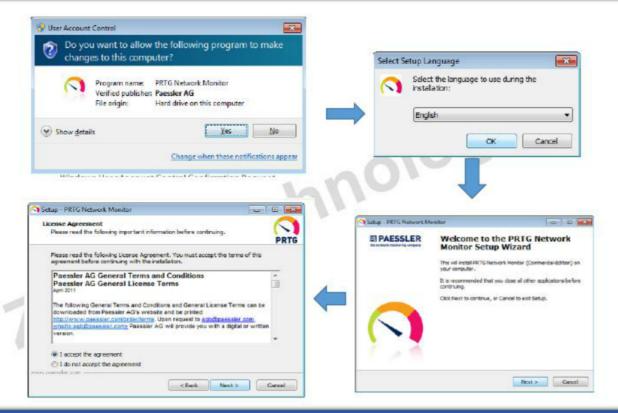


PRTG is network monitoring software from Paessler AG. PRTG runs on Windows and monitors network availability and network usage using SNMP, Packet Sniffing, WMI, IP SLAs and Netflow and various other protocols.



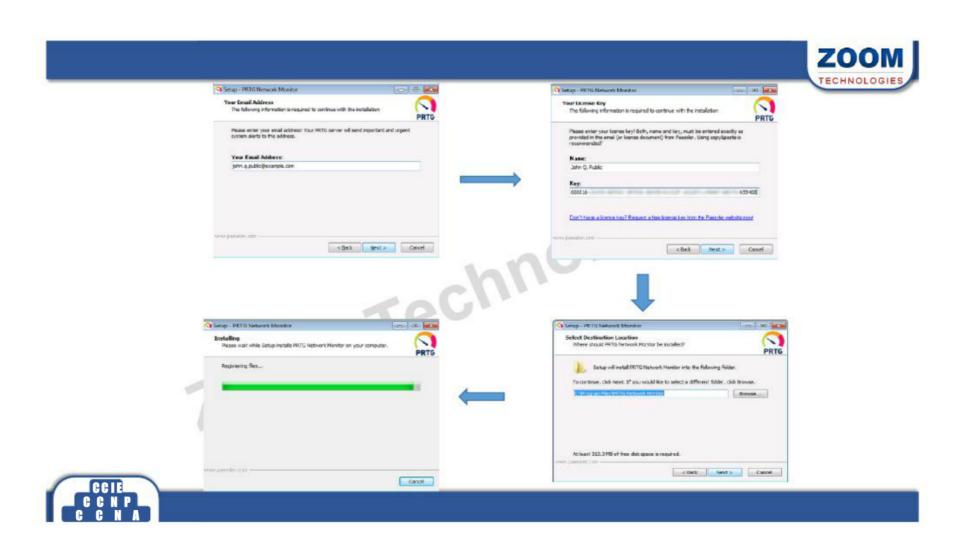
#### Installation.....

















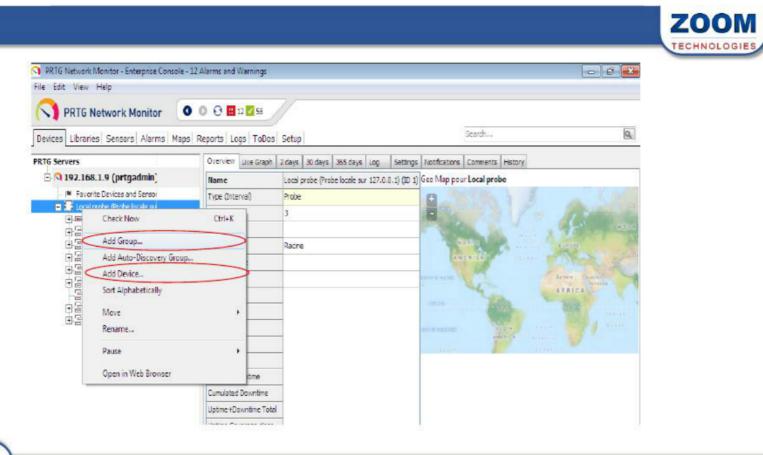
#### **How It Works?**







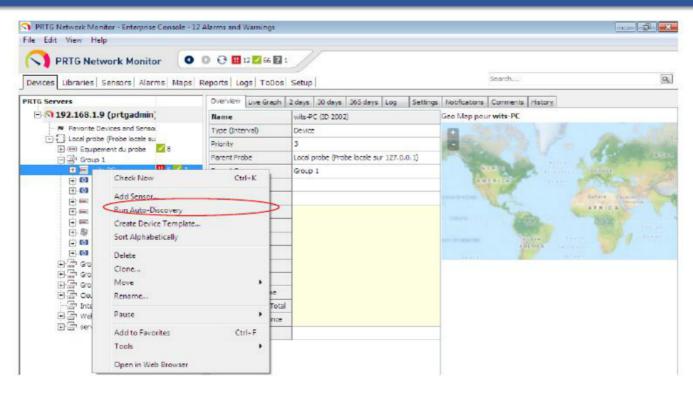
TECHNOLOGIES













#### Why Network Monitoring?

















- PRTG Network Monitor consists of different parts which can be divided into three main categories: Technologies
- **System parts** 
  - **Core Server**
  - Probe(s)
- **Control interfaces** 
  - **Ajax Web Interface**
  - **Enterprise Console**
  - **Mobile Web GUI**
  - **Smart Phone Apps**







- **Basic administration interfaces**
- Zoom Technologies PRTG Server Administrator
- PRTG Probe Administrator



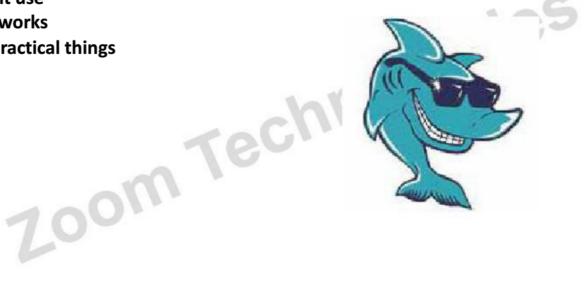




## **Agenda**



- What is Wireshark
- Where it use
- How it works
- Some practical things







· Network analysis is the process of capturing network traffic and inspecting it closely to Zoom Technologies determine what is happening on the network.





#### What is Wireshark.....?



- Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- Previously the packet analyzing was very difficult and it required expensive hardware.
- Wireshark is one of the best open source packet analyzer available.
- A packet analyzer is also known as a sniffer, network analyzer or protocol analyzer.



#### Who and where is tool is use ...?



gies

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- · People use it to learn network protocol internals

700m

Beside these examples Wireshark can be helpful in many other situations too.







## **Shark on Water**







## Shark on wire







#### How it works?

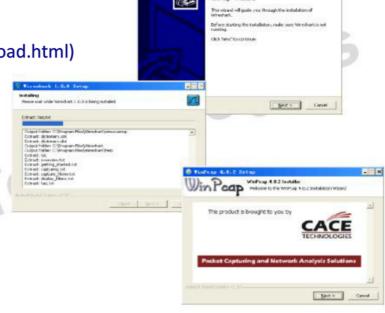


#### **For Windows**

download (http://www.wireshark.org/download.html)

install

- use





## WIRESHARK

Zoom

#### **Installation Process**



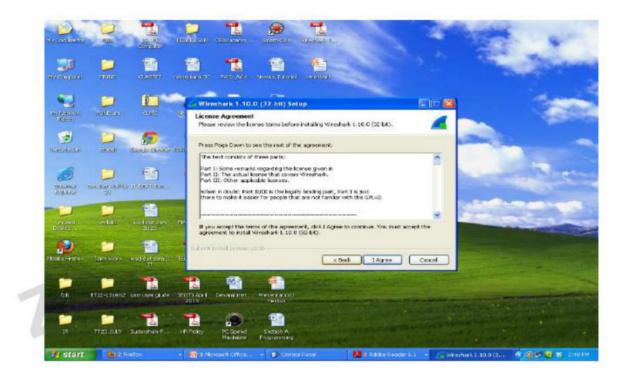








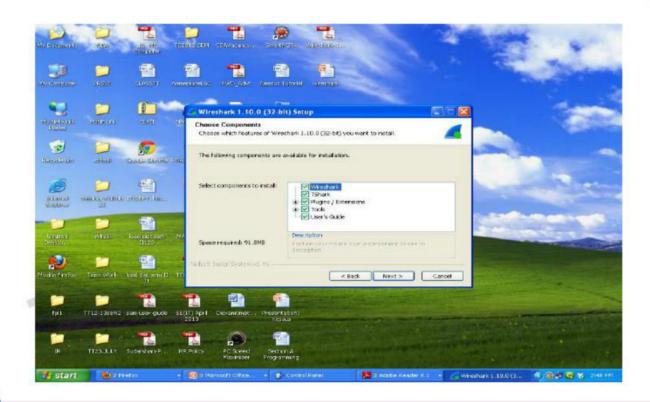
#### STEP 2:







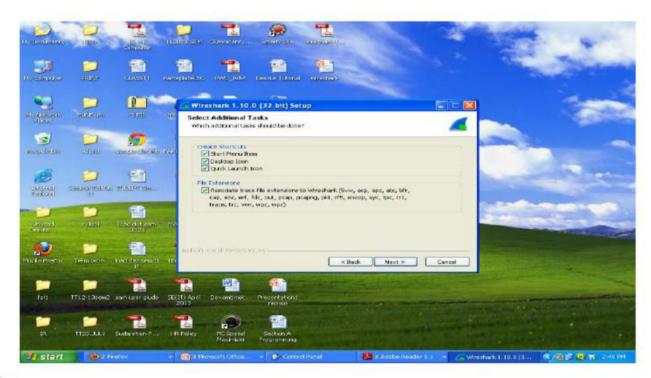
#### STEP 3:





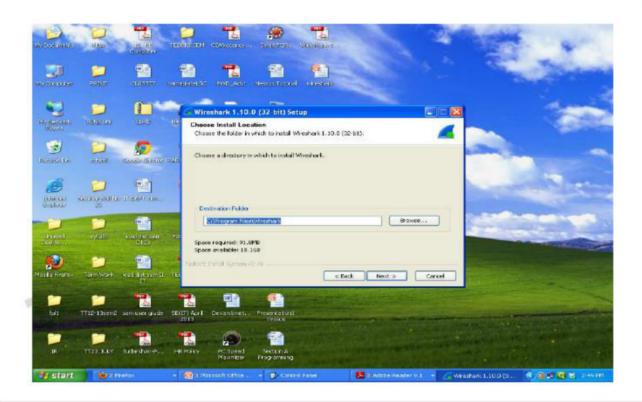








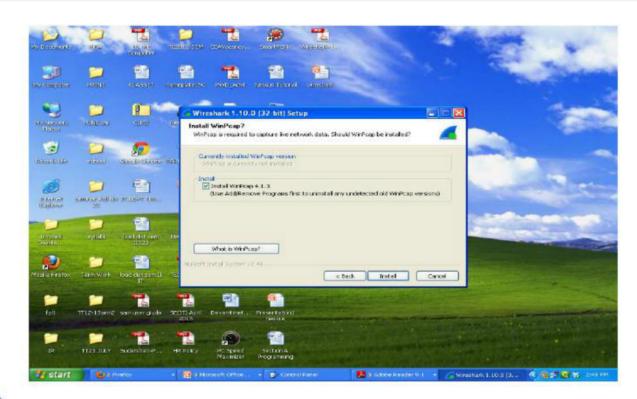
# ZOOM





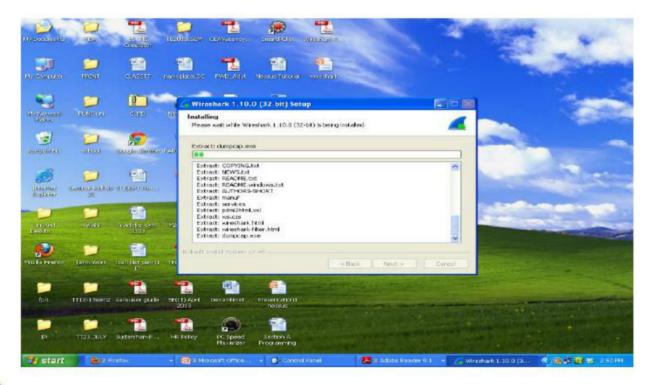








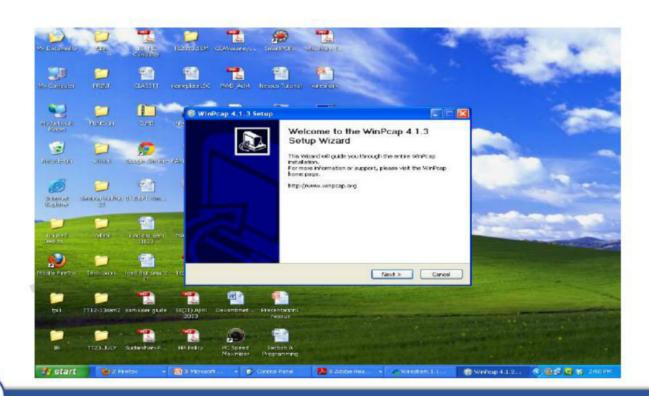
# ZOOM













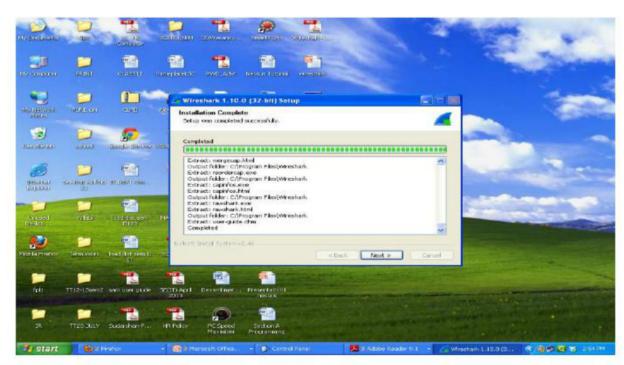






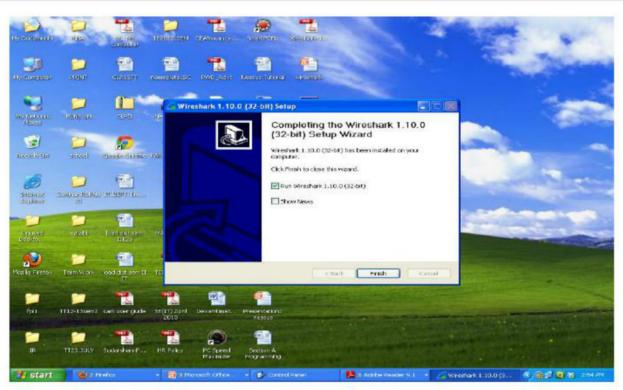








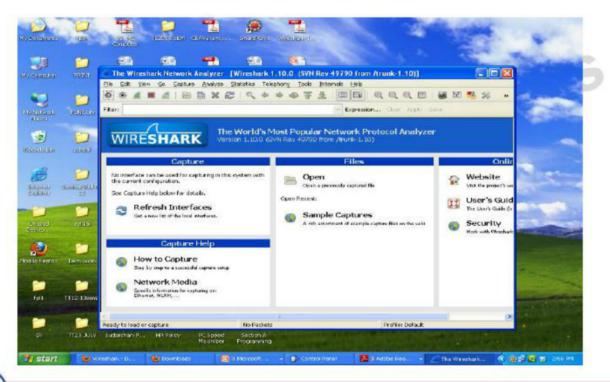
## ZOOM













#### **Wireshark Graphical User Interface**



When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will de displayed. Initially, no data will be displayed in the various windows.

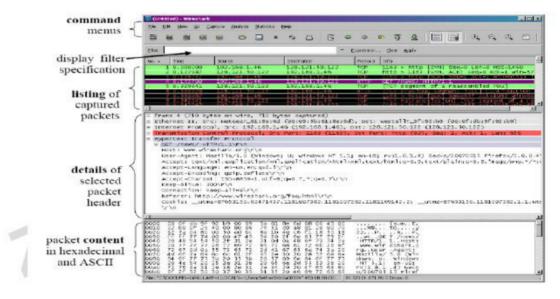
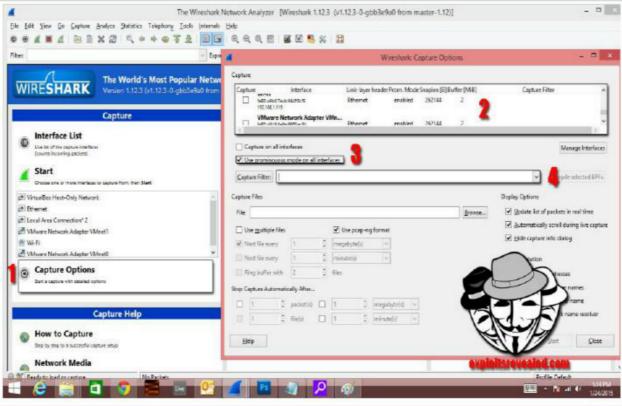


Figure 2: Wireshark Graphical User Interface







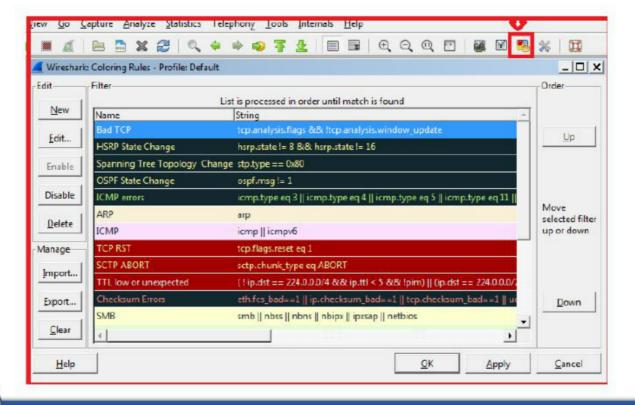




CCIE

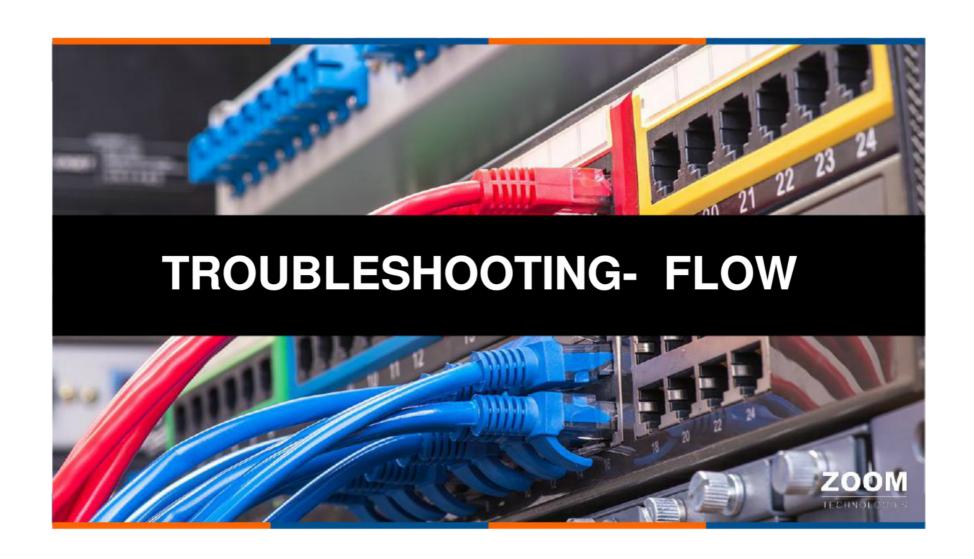
#### **WIRESHARK COLOR CODED**











**Troubleshooting Flow** 



Problem Reporting

Problem Diagnosis

Problem Resolution



#### **Popular Troubleshooting Methods**

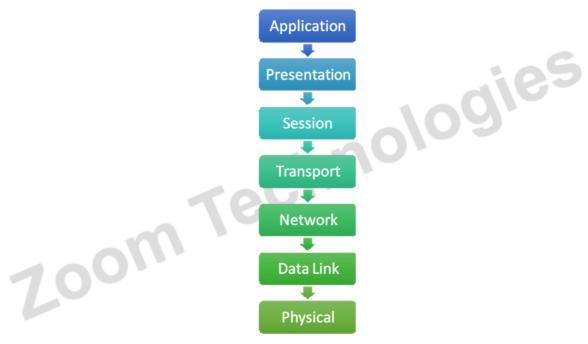


- Top-down method
- Bottom-up method
- Zoom Technologies Divide and Conquer method
- Following the Traffic path
- Comparing configurations
- Component swapping



#### Top-down method



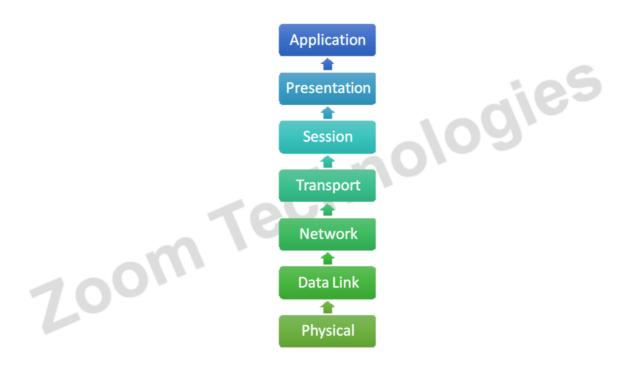






#### **Bottom Up method**

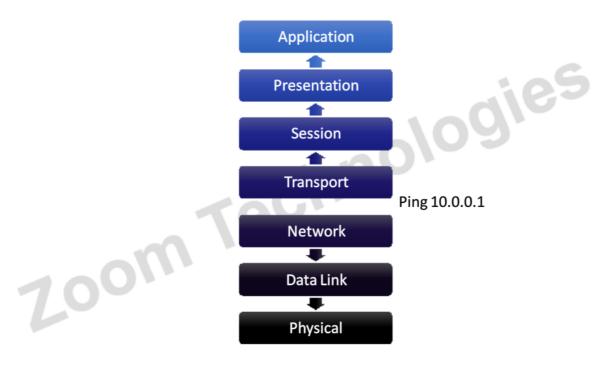






#### **Divide and Conquer**



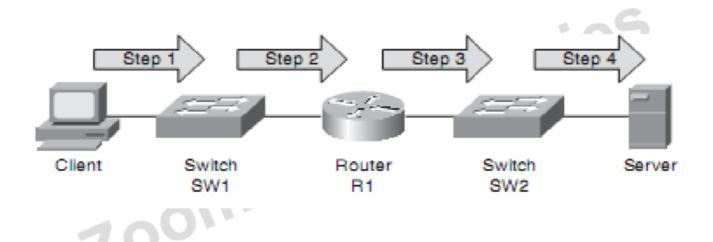






## Follow the Traffic path method

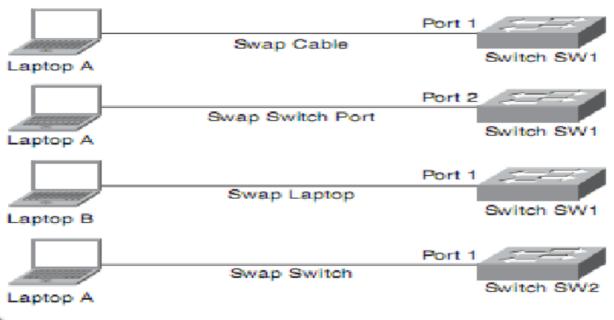






#### **Component swapping**









#### **Network Maintenance**



- What is Network Maintenance?
  - Doing whatever is required to keep the network functioning and meeting the business needs of an organization.
- It is a very important responsibility or duty of the Network Administrator
- It could also be a response to a reported problem
- ... maint Proactively performing regular scheduled maintenance tasks reduces problems



#### **Basic Network maintenance toolkit**



- CLI Tools
- GUI Tools
- Backup tools
- Logging Tools
- Network Time Protocol
- Zoom Technologies Network Documentation Tools





#### **Examples of Network Maintenance**



gies

- Hardware and Software installation and configuration
- Monitoring and Tuning Network performance
- Network expansion planning
- Documentation of Network changes
- Compliance with legal regulations and corporate policies
- z exte Securing the Network from Internal and External threats



#### **Common Elements in Network Documentation**



- Logical Topology Diagram
- Physical Topology Diagram
- Interconnections list
- 7.00m Technologies Inventory of Network equipment
- IP Address Assignment
- Configuration Information
- Original Design Document

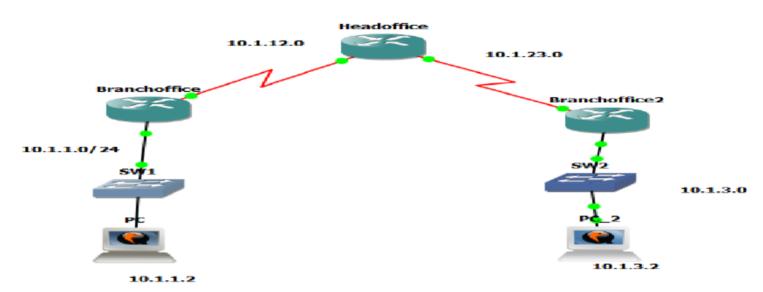






## **EIGRP Troubleshooting**





User working in BranchOffice 1 is not able to communicate with user in Branch Office 2





### **EIGRP Troubleshooting**

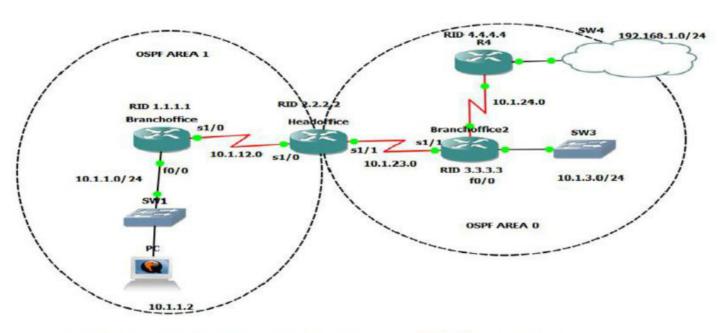


- · Interface is down
- oom Technologies Mismatched Autonomous Systems
- Incorrect Network Statement
- Mismatched K Values
- Passive Interface
- Different Subnet
- Authentication
- ACI
- Timers



#### **OSPF Troubleshooting**





users in branchoffice 1 are not able to access the resources 192.168,1.0/24 network





#### **OSPF Troubleshooting**



- Interface is down
- Zoom Technologies · Interface not running the OSPF process.
- Mismatched timers.
- · Mismatched area numbers
- Mismatched area type



#### **OSPF Troubleshooting**



- Different subnets
- Passive interface
- .,pes Mismatched authentication
- ACL
- MTU mismatch
- Duplicate Router ID
- Mismatched network types





#### **OSPF** troubleshooting



- MTU mismatch:
- The maximum transmission unit of neighboring interfaces must match.
- · Deliberately configure a different MTU on interfaces of two routers sharing a link

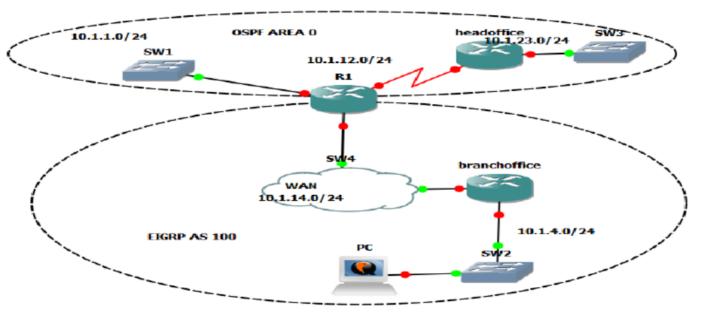
hnologi

- Router(config)#int s1/0
- Router(config-if)#ip mtu 100
- Verify
- Router#Sh run interfaces s1/0
- · After configuring verify by giving the neighbor command
- The state will be exstart



#### Redistribution





Users from branchoffice cannot communicate with any resources out side the branchoffice





#### Redistribution

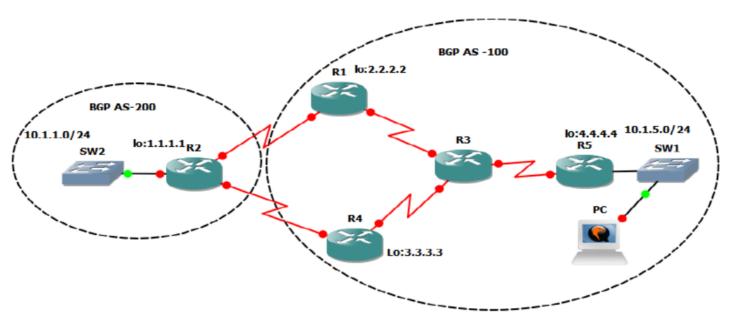


- Distribute list
- Zoom Technologies Route-maps
- Metric
- AS number
- Process-id
- Hop count



#### **BGP Troubleshooting**





you are the administrator for AS-100 ,the users from 10.1.1.0/24 network is not able to communicate to 10.1.5.0/24





#### **BGP Troubleshooting**



- · Interface is down
- · Layer 3 connectivity is broken
- Incorrect neighbor statement
- · Incorrect network command
- Zoom Technologies BGP packets are sourced from wrong IP address
- · Mismatched of Authentication
- Neighbor doesn't have a route



#### **BGP Troubleshooting**

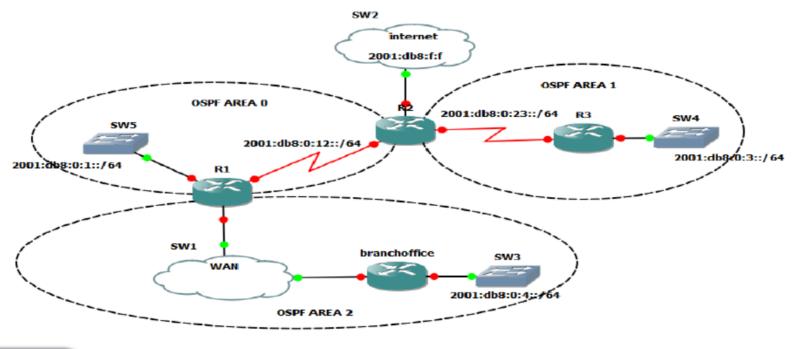


- Zoom Technologies Next hop router is not reachable
- BGP Split horizon
- BGP Synchronization
- Route Filtering







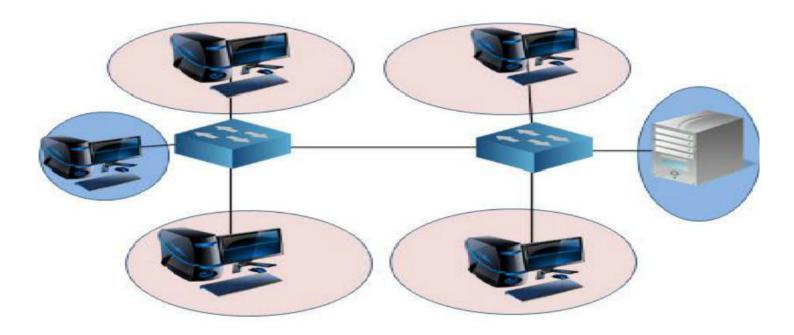






## **Troubleshooting Trunks**







## **Troubleshooting Trunks**

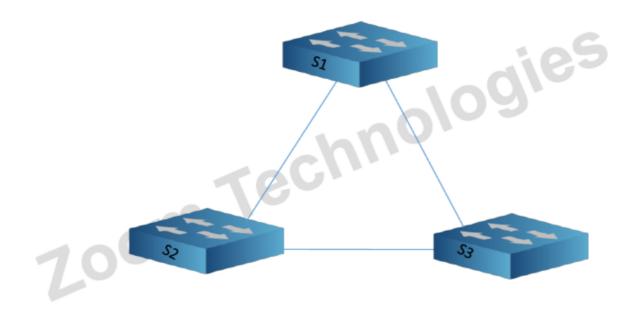


- Encapsulation Mismatch
- Zoom Technologies Incompatible Trunking modes
- Native Vlan Mismatch
- Allowed vlans
- · VTP domain name mismatch











#### **VTP Troubleshooting**



- Domain name mismatch
- Version mismatch
- Mode mismatch
- Zoom Technologies Password mismatch





#### VTP domain name mismatch



- Sw\_server(config) vtp domain zoom.com
- Sw\_client(config) vtp domain zoom.com

Note: the domain name is only propagated in the beginning if it is null then it will join the first domain but when it is already part of a domain then it won't update the ally als domain name. That has to be done manually also on the clients.



#### **VTP Troubleshooting**



- Domain name mismatch
- Version mismatch
- Mode mismatch
- Zoom Technologies Password mismatch





## **Troubleshooting VLANS**

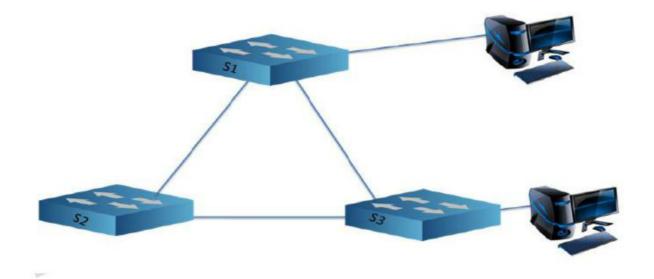


- Incorrect IP address
- Missing vlan
- Zoom Technologies Incorrect port Assignment

# CCIE CCNP CCNA

## **STP Troubleshooting**









## **STP Troubleshooting**

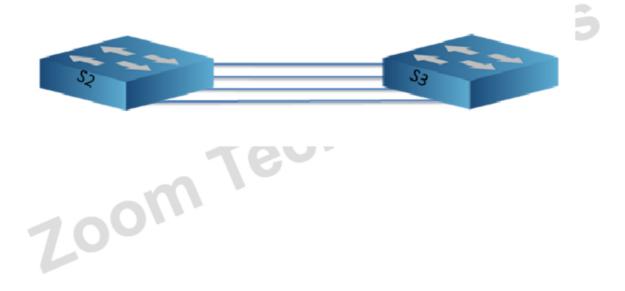


- · No Trunking connectivity
- STP disabled
- Portfast
- Zoom Technologies · BPDU Guard and BPDU filter
- Loop Guard



#### **ETHERCHANNEL Troubleshooting**









### **ETHERCHANNEL Troubleshooting**

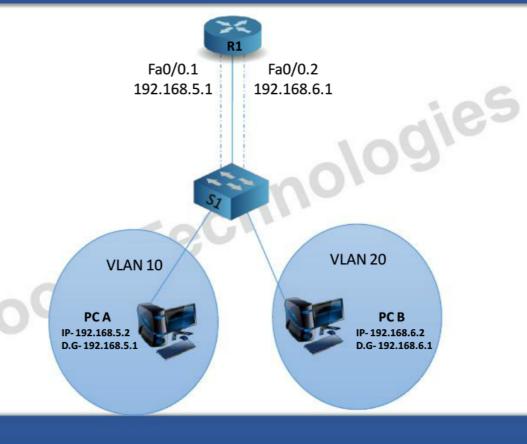


- Mismatched Port configurations
- Zoom Technologies Mismatched Etherchannel Configuration
- Mismatch of Protocol



### **Inter Vlan Routing Troubleshooting**

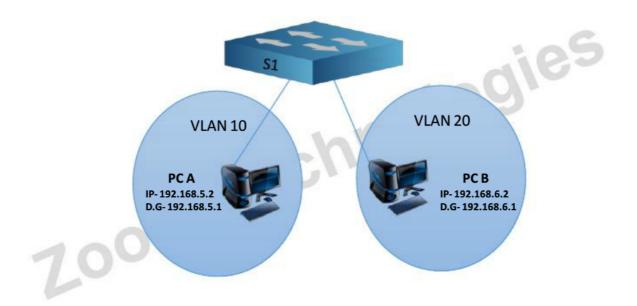






# **Inter Vlan Routing Troubleshooting**

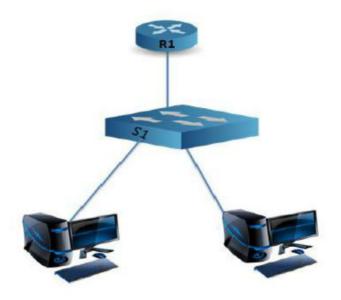






# **Switch Security**









### **Switch Security Troubleshooting**



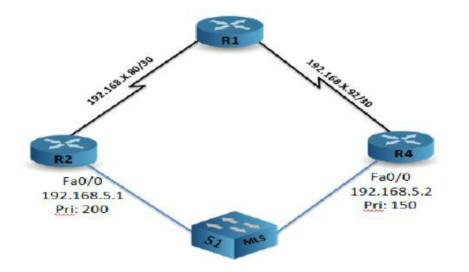
- · Port security configured but not enabled
- A static MAC address was not configured correctly
- The maximum number of MAC addresses has been reached ,preventing access
- Legitimate users are being blocked because of violation
- Running configuration not saved to startup configuration



#### **Troubleshooting FHRP**

1









## **FHRP Troubleshooting**



- Group number
- Zoom Technologies · Same virtual IP address
- Priority
- Preemption
- Interface tracking



# CSE-2012 Full Course

#### MICROSOFT CERTIFIED SOLUTIONS EXPERT

Practicals in real-time environment. Detailed curriculum with all 5 papers **Duration: 1 Month | 4 Hrs Per Day** (starts on 15th & 30th of every month) Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

# (v 2.0) Full Course

#### CISCO CERTIFIED NETWORK ASSOCIATE

Cisco Routers with BSNL/TELCO MUX & Live Channelised E1 **Duration: 1 Month | 4 Hrs Per Day** (starts on 15th & 30th of every month) **Batches:** Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

# 18181841

## COMPLETE RHCE LINUX

Practicals on Live Web Administration + Integration of Windows with Linux/Unix (Samba Server) **Duration: 2 Weeks | 4 Hrs Per Day** (starts on 15th & 30th of every month)

Batches: Morning: 8.00 ● Afternoon: 1.30 ● Evening: 7.00

- Ethical Hacking, Cyber Security and Firewall Open Source: A glimpse into advance Linux VMware vSphere and MS Private Cloude Cisco WAN Technology & Collaboration

Free MCSE & CCNA Exam Practice Questions

# **Ethical Hacking & Countermeasures Expert**

Course is mapped to EHCE course from US-Council (www.us-council.com) (Pre requisite is CCNA / MCSE / LINUX)

**Duration: 2 Weeks | 4 Hrs Per Day** (starts on 15th & 30th of every month) Batches: Morning: 7.30 or Evening: 6.00

Complete Package for Only

Fees: ₹ 5,900/-

+ 14% Service Tax **Duration: 3 Months** 4 Hrs Per Day

> 100% GUARANTEED

> > **ASSISTANCE**

# R&S

#### CISCO CERTIFIED NETWORK PROFESSIONAL

**Duration: 1 Month | 4 Hrs Per Day** (starts on 15th of every month) Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 6.00

Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

• PRTG • Wireshark • SolarWinds, etc.

**Exam Practice Challenge Labs** 

#### CISCO CERTIFIED INTERNETWORK EXPERT

**Duration: 1 Month | 4 Hrs Per Day** (starts on 15th of every month)

Individual Rack For Every Student
 Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

### Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

**Unlimited Lab Access For 1 Year** 

Fees: ₹ 10,000/-**Introductory Special Offer** 

Fees: ₹ 9,500/-

+ 14% Service Tax

Fees: ₹ 5.500/-

+ 14% Service Tax

Fees: ₹ 25,000/-Introductory Special Offer

+ 14% Service Tax

# MICROSOFT EXCHANGE SERVER-2013

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month) **Batches:** (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-+ 14% Service Tax

Microsoft Certified Solutions Expert [MCSE] Private Cloud

**Duration: 2 Weeks | 4 Hrs Per Day** 

**Batches:** (Contact the Counselors for the next available batch)

Fees: 2,500/-+ 14% Service Tax

# VANCED LINUX

**Duration: 2 Weeks | 4 Hrs Per Day** (starts on 15th & 30th of every month) **Batches:** (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-+ 14% Service Tax

(Pre requisite is CCNA R&S)

CISCO CERTIFIED NETWORK ASSOCIATE - SECURITY

**Duration: 2 Weeks | 4 Hrs Per Day** (starts on 15th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹7,500/-+ 14% Service Tax

(Pre requisite is CCNA Security at ZOOM)

CISCO CERTIFIED NETWORK PROFESSIONAL - SECURITY

**Duration: 2 Weeks | 4 Hrs Per Day** (starts on 30<sup>th</sup> of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹9,500/-+ 14% Service Tax

(Pre requisite is CCNA & CCNP Security at ZOOM)

CISCO CERTIFIED INTERNETWORK - SECURITY

Duration: 1 Month | 4 Hrs Per Day

**Batches:** (Contact the Counselors for the next available batch)

Fees:₹15,500/-+ 14% Service Tax

# VMware vsphere (Pre requisite is MCSE)

**Duration: 1 Month | 4 Hrs Per Day** (starts on 15th of every month)

Batches: Morning: 7.30 and Evening: 7.30

Fees: ₹ 4,950/-+ 14% Service Tax

# VMWare vSphere)

**Duration: 1 Week | 4 Hrs Per Day** (starts on 15th of every month)

Batches: Morning: 9.30 to 11.30

Fees: ₹ 2,500/-+ 14% Service Tax

**Duration: 2 Weeks | 4 Hrs Per Day** 

Batches: (Contact the Counselors for the next available batch)

Fees: ₹5,500/-+ 14% Service Tax

We also offer the following courses (Contact the Counselors for the next available batch)

- CCNA Voice
- **@ ₹7,500/-**
- , CCNA Data Center @ ₹7,500/-

- CCNP Voice
- **@ ₹9,500/-**
- CCNP Data Center @ ₹9,500/-
- CCIE Collaboration @ ₹15,500/-
- CCIE Data Center **@**₹15,500/-

IPv6 Migration @ ₹5,500/-

# FACULTY

- All Senior Engineers of Zoom working on Live projects
- Training Engineers of British Army, CISCO, CMC, GE, BSNL, Tata Teleservices and Several Corporates etc for 18 Years.

# **FREE Training**

Zoom Technologies offers a number of free resources for the professional development of network engineers.

Register on our website to get access to the video recordings of live sessions on:

- MCSE Windows Server 2012
- Cisco CCNA `
- Cisco CCIE
- Exchange Server 2013
- LinuxL
- All Flavors

  Advanced Linux
- Ethical Hacking and Countermeasure Expert (www.us-council.com)

### Find us at: www.zoomgroup.com

Like us on Facebook and get access to free online webinars as well as special offers and discounts. https://www.facebook.com/ZoomTechnolgies

# **Online Training**

Online Training at Zoom is a cost effective method of learning new networking skills from the convenience of your home or workplace.

Taking an online training course has many advantages for everyone (Freshers / Working Professionals). Zoom offers online training for the highly coveted CCNA, CCNP and CCIE courses as well as MCSE, Linux, VMware, Ethical Hacking and Firewalls, IPv6 with more courses planned for the near future. These are live instructor led courses, using Cisco WebEX. Check out our online course offerings at: http://zoomgroup.com/online\_course

# **Job Opportunities**

There is a high demand for network and security professionals at all times. Apart from job opportunities in India and the Middle East, network and security administrators are also sought-after in the US and Europe.

If you do not have the right skills, then get them now! Choose the experts in network and security training, an organization which has already trained over one hundred thousand engineers.

For the latest job openings in networking and security, register and upload your resume on: **http://zoomgroup.com/careers** or visit zoom to choose job offering from several multinational companies.

### **ABOUT US**

**ZOOM** Technologies India Pvt. Ltd. is a pioneering leader in network and security training, having trained over a hundred thousand engineers over the last two decades.

We offer a world class learning environment, with state-of-the-art labs which are fully equipped with high-end routers, firewalls, servers and switches. All our courses are hands-on so you'll get much needed practical experience.

The difference between us and the competition can be summed up in one simple sentence. Our instructors are real-time network professionals who also teach.

Zoom has designed, developed and provided network and security solutions as well as training to all the big names in the Indian industry, for the public sector as well as corporate leaders. Some of our clients are:

TATA
BSNL
VSNL
Indian Railways
National Police Academy
Air Force Academy
IPCL- Reliance Corporation
CMC
British Army

No other training institute can boast of a customer base like this. This is the reason for the resounding success of our networking courses. If you do not have the right skills, then get them now. Come, join the experts!

# Training Centers in Hyderabad, India.

### **Banjara Hills**

HDFC Bank Building, 2nd Floor, Road # 12, Banjara Hills, Hyderabad - 500 034 Telangana, India.

Phone: +91 40 23394150 Email: banjara@zoomgroup.com

#### **Ameerpet**

# 203, 2nd Floor,
HUDA Maitrivanam, Ameerpet,
Hyderabad - 500 016
Telangana,
India.

Phone: +91 40 39185252 Email: ameerpet@zoomgroup.com

#### Secunderabad

Navketan Building, 5 Floor, # 501 Secunderabad - 500 003 Telangana, India.

Phone: +91 40 27802461 Email: mktg@zoomgroup.com

### Dilsukhnagar

Ist Floor, # 16-11-477/B/1&B/2, Shlivahana Nagar, Dilsukhnagar, Hyderabad - 500 060 Telangana, India.

Phone: +91-40-24140011 Email: dsnr@zoomgroup.com

website: www.zoomgroup.com